Due diligence in cyberspace: guidelines for international and European cyber policy and cybersecurity policy

Bendiek, Annegret

Veröffentlichungsversion / Published Version
Arbeitspapier / working paper

Zur Verfügung gestellt in Kooperation mit / provided in cooperation with:
Stiftung Wissenschaft und Politik (SWP)

Empfohlene Zitierung / Suggested Citation:
Bendiek, A. (2016). *Due diligence in cyberspace: guidelines for international and European cyber policy and cybersecurity policy.* (SWP Research Paper, 7/2016). Berlin: Stiftung Wissenschaft und Politik -SWP- Deutsches Institut für Internationale Politik und Sicherheit. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-47152-8

SWP Research Paper
Stiftung Wissenschaft und Politik
German Institute for International
and Security Affairs

Annegret Bendiek

Due Diligence in Cyberspace

Guidelines for International and European Cyber Policy and Cybersecurity Policy

RP 7
May 2016
Berlin

SWP Research Papers are
peer reviewed by senior
researchers and the execu-
tive board of the Institute.
They reflect the views of
the author(s).

SWP
Stiftung Wissenschaft
und Politik
German Institute
for International
and Security Affairs

Ludwigkirchplatz 3–4
10719 Berlin
Germany
Phone +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

ISSN 1863-1053

Translation by Tom Genrich

(English version of
SWP-Studie 3/2016)

Table of Contents

Dr Annegret Bendiek is a Senior Associate in SWP's EU/Europe Division.
This study emerged out of the project "The challenges of digitalisation for Germany's foreign and security policies", which was financially supported by the Planning Staff of the German Ministry for Foreign Affairs.

Due Diligence in Cyberspace
Guidelines for International and European Cyber Policy and Cybersecurity Policy

Global cyberspace is undergoing fundamental change. There are now frequent references to a "fragmentation of the Internet", but many European and international working groups are also increasingly aware that "a free, open and at the same time secure Internet" is a global public good. To create and preserve the Internet as a public good, concerted global action is needed on the basis of a common norm, which makes states mutually responsible for their diligence in national regulatory processes. This norm is implicitly incorporated in the German cybersecurity strategy of 2011 as well as the EU's 2013 cybersecurity strategy, which provides for civil, police and military-defensive approaches to protecting information-technology (IT) systems and infrastructure.

In the course of the discussion about a new German cybersecurity strategy to be adopted in late autumn of this year, a growing number of political voices have also argued that political regulation and digital sovereignty should be strengthened and renationalised. Politics must face up to the reality of the military becoming increasingly operative in cyberspace. This will be reflected in the German Federal Government's new White Paper as well as in NATO's and the EU's future cyberdefence. In other words, it will be implemented in the German and European security policy as well as in their defence missions and military procurement.

Liberal democracies need to be aware that the idea of a free and open Internet can only be realized if there is consensus among a "coalition of liberal states" not only on how the Internet should be governend but why International and transatlantic cooperation is meaningful. German and European policy should go ahead and orientate itself on the norm of due diligence in cyberspace – and do so in an interministerial way – so as to enforce it internationally. Due diligence in cyberspace builds on the international legal standard of due diligence, which stipulates that a state must do everything necessary to prevent actions emanating from within its own territory that might infringe the rights of third parties. In the Organisation for Economic Cooperation and Development (OECD), for instance, there is far-reaching consensus on due diligence, which would be an obvious choice for the

normative basis for a global cyber order. The political rules adopted for an international cyber policy and cybersecurity policy will always lag behind technological developments. It is the more important, therefore, that new regulations be subordinated to an overarching norm. Three crucial political requirements arise from this:

- European cooperation: integrating national policies into the European framework;
- Inclusiveness: giving different interest groups broad and publicly accessible representation in formulating policies;
- Civilian response: prioritising the civilian component over the military component, particularly in times of peace.

European cooperation. Due diligence demands that states behave responsibly not only towards one another, but also in internal and home affairs regulatory practices. The EU's 2013 cybersecurity strategy already provided for this. As part of implementing the EU directive on network and information security (NIS), all EU states must introduce minimum standards and reporting requirements for IT security, and operators of critical infrastructure must be involved in fighting cybercrime. To establish the digital single market, national regulations in civil law (data protection), commercial law (Internet Governance) and competition law (domestic market) must be worded in such a way as to fulfil due diligence obligations. To accelerate this process, it will be advisable quickly to pass the EU's planned Global Strategy for cyberspace. NATO and EU members largely agree that states are responsible for their own behaviour in cyberspace. There is close consultation among Europe's "Big Three" on all of these issues, as well as with the group of likeminded western states. European and western states represented in the United Nations Group of Governmental Experts (UN GGE) should use the upcoming fifth round of UN GGE negotiatons to campaign for the fight against cybercrime, by adapting their substantive criminal law. The minimum conditions for global cybersecurity are ratifying the Budapest Convention on Cybercrime as well as continuous confidence- and security-building measures (CSBM) in the Organisation for Security and Cooperation in Europe (OSCE).

Inclusiveness. The UN summit in December 2015, which was part of the WSIS (World Summit on the Information Society) follow-up process, showed that a worldwide agreement on a binding interpretation of due diligence is unlikely in the short term. Therefore, the decision taken in December 2015 to continue the Internet Governance Forum – in other words, to keep pursuing the multi-stakeholder approach – still offers the best chance of preventing the idea of a global free and open Internet from falling victim to governments' intensifying security considerations. In Internet Governance, it is therefore crucial to support the multi-stakeholder approach (interpreted inclusively) and to reject the principle of intergovernmental decision-making. The experience of the WSIS process of the past ten years has clearly shown the ineffectiveness of intergovernmental decision-making. In addition, it would be important to make the norm of due diligence binding on all stakeholders: private users, access-network operators and operators of transmission networks and Internet exchanges. In the long term, arbitration authorities ought to ensure that due diligence is properly implemented.

Civilian response. Initiatives such as a national strategy to protect the economy and industry against espionage back strengthened defensive intelligence capabilities. However, the German Ministry of Defense indicates that it wants to build additional defensive capabilities for reacting to cyber attacks. It would not be advisable for the government to evolve towards an offensive cyberdefence. That would not only be in open contradiction with the idea of due diligence in cyberdiplomacy, but it would also bring with it the risk of conflict escalation and a proliferation of cyber attacks. It is common sense that cyber attacks are difficult to attribute and retaliatory attacks can cause serious unintended damage. The June 2015 attack on the German Federal Parliament showed how vital it is to persist in developing resilient structures. Declaring a given act a violation of sovereignty; having recourse to NATO solidarity; or declaring cyberwar against Islamic State, as the US did, must be seen as the last resorts of politics. Further resources are necessary to prop up a strategy based on resilience: for high-security technology, for developing digital forensics, and for extensive further-training measures to heighten awareness among civil servants, scientists, academics and researchers. Confidence-building measures within the OSCE, capacity-building in third countries under the leadership of the EU and the GGE must be intensified. This is the only realistic basis for achieving bilateral agreements that improve cooperation in solving and prosecuting cross-border digital crimes and remove so-called "safe havens". A recent example of this is the accord between the US and China on fighting cybercrime.

Due Diligence as a Guiding Principle

> "Cybersecurity due diligence has been defined as the review of the governance, processes and controls that are used to secure information assets. Or more simply, due diligence refers to your activities to identify and understand the risks facing your organization. Such due diligence obligations may exist between states, between non-state actors (e.g., private corporations), and between state and non-state actors. Here the term is used to refer to the international obligations of both state and non-state actors to help identify and instil cybersecurity best practices so as to promote the security of critical ICT infrastructure."[1]

European and German cyberdiplomacy aim to "protect and further an open, free and secure global Internet as a space for diversity of opinions, participation, innovation and engine for economic growth and work".[2] This can also be described as a global public good, whose provision requires the cooperation of all important states, businesses, academics and civil society.[3] It will only be possible to prevent regional fragmentation, the threat of crime and a militarisation of cyberspace[4] if the community of states – including all Internet stakeholders[5] – agrees on common norms of conduct and accepts rules that make these norms binding. Cybersecurity, in other words, is the "state of IT security to strive for, at which the risks of global cyberspace are reduced to an acceptable level".[6]

The German federal government, EU member states and the EU itself adhere on principle to the idea of "due diligence"[7] in implementing their cybersecurity strategies.[8] This norm commits states to ensuring that no actions originating on their territory in times of peace violate the rights of other states.[9] In its cybersecurity strategy, the German Federal Government foregrounded the preventative and reactive protection of IT systems and infrastructures as well as civilian, police and military-defensive approaches. Further-

1 Scott J. Shackelford, talk given to the CyberLab of the Stiftung Wissenschaft und Politik (SWP) (Brussels, November 2015).

2 German Federal Government, *Europäische und internationale Dimension der Digitalen Agenda*, http://www.digitale-agenda.de/Webs/DA/DE/Handlungsfelder/7_Dimension/dimension_node.html (accessed 30 November 2015).

3 Important suggestions for this pilot study came from working-group results from two events: the SWP's CyberLabs with about 60 participants, held in the offices of the Stiftung Wissenschaft und Politik in Berlin (8 September 2015), and the Permanent Representation of the Federal Republic of Germany to the European Union in Brussels (18 November 2015). I am particularly grateful to Prof. Christopher Daase (Goethe University, Frankfurt/Main) as well as to Prof. Scott Shackelford (Indiana University, Bloomington, USA) and to all participants from the executive and legislative branches and other stakeholders for their constructive collaboration.

4 The German Federal Government's cybersecurity strategy states: "Cyberspace is the virtual space of all IT systems networked at the data level on a global scale. Cyberspace is based on the universal and publicly accessible connection and transport network of the Internet, which can be complemented and expanded at will by other data networks. IT systems functioning in an isolated virtual space are not part of cyberspace." German Federal Ministry of the Interior, ed., *Cyber-Sicherheitsstrategie für Deutschland* (Berlin, 2011), 14, http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf?__blob=publicationFile.

5 "The Internet is a worldwide web of publicly accessible networks. These networks are operated independently of each other, but use a joint address space and standardised joint 'languages', so-called transmission protocols, to ensure mutual accessibility. The Internet Protocol (IP) in particular has a crucial role. The internet makes it possible to transport data at will." Jens Tiemann and Gabriele Goldacker, *Vernetzung als Infrastruktur – Ein Internet-Modell* (Berlin: Kompetenzzentrum Öffentliche Informationstechnologie [ÖFIT], October 2015), 10, http://www.oeffentliche-it.de/documents/10181/14412/Vernetzung+als+Infrastruktur+-+Ein+Internet-Modell (accessed 5 February 2016).

6 German Federal Ministry of the Interior, ed., *Cyber-Sicherheitsstrategie für Deutschland* (see note 4), 15; Hans-Jürgen Lange and Astrid Bötticher, eds., *Cyber-Sicherheit* (Wiesbaden: Springer VS, 2015).

7 The principle of due diligence derives from a verdict of the International Court: International Court of Justice, *United Kingdom of Great Britain and Northern Ireland v. Albania, The Corfu Channel Case (Merits), Judgment of April 9th, 1949*, 4–38.

8 For the application of this concept to cybersecurity, see Scott Shackelford, Scott Russell and Andreas Kuehn, *Unpacking the International Law on Cybersecurity Due Diligence: Lessons From the Public and Private Sectors*, Kelley School of Business Research Paper no. 15–64 (Bloomington: Indiana University, 27 August 2015).

9 Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York: Cambridge University Press, 2013); German Federal Ministry of the Interior, ed., *Cyber-Sicherheitsstrategie für Deutschland* (see note 4), 12.

more, the International Court has elaborated in a decision "that the obligation of prevention is a due diligence obligation".[10] Due diligence enables the international community to use international law "to hold states to account for omissions in making their infrastructure safe; for breaching their obligations by neglecting to take action; or for a lack of cooperation in protecting against and solving cyber attacks".[11]

In 2000, the UN General Assembly called on states „[to] ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies".[12] The UN Group of Governmental Experts (GGE), in which Germany is represented, picked up this idea in its final report of June 2015. According to the report, all states shall ensure that their territories, and especially the computersystems and infrastructure situated there or otherwise under the states' control, is not misused for attacks on the infrastructure of other states.[13]

Due diligence is usually translated in international law treaties by the rather problematic term "Sorgfaltspflicht".[14] However, this term only refers to restrictions on one's own conduct. It is therefore more meaningful to use "Sorgfaltsverantwortung" for due diligence. The principle of due diligence derives its particular normative force from the idea that states are not only responsible for keeping law and order on their own territories, but also *bear responsibility for the external consequences of internal regulations*. Decisions taken by individual states increasingly have an impact beyond their national territory. That is why states must exercise care with such decisions and be accountable to one another for them. As far as cyberspace is concerned, states may not simply limit themselves to taking no irresponsible decisions. This study further assumes that safeguarding the Internet needs to the political will by all stakeholders for international cooperation.[15] Accordingly, states in cooperation with other states are obliged to do everything that may be reasonably expected of them to help deliver an "open, free and secure Internet".

This expectation encompasses decision-making processes that meet high standards. This means that available competences should be integrated as far as possible, and that one-sided interest-driven politics should be avoided.[16] In other words, an international cyber policy and cybersecurity policy defined by due diligence necessarily also comprises the specific mode of regulation. Germany's international cyber policy and cybersecurity policy thus needs to be coordinated at the European level, militarily reticent, and integrated into inclusive and transparent regulatory processes.[17]

- Due diligence[18] comprises regulatory processes with a high level of representativity and inclusiveness as well as transparency. As Christopher Daase pointed out: "In democracies, in the long term, no policy can be pushed through against the will of the majority and not even against the resistance of

10 International Court of Justice, "Case Concerning Pulp Mills on the River Uruguay (Argentina v. Uruguay), Judgment, 20 April 2010", *ICJ Reports* 79 (2010): 14–107. [Paragraph 197]: "the obligation [...] to prevent [...] is an obligation to act with due diligence in respect of all activities which take place under the jurisdiction and control of each party".

11 Christian Schaller, *Internationale Sicherheit und Völkerrecht im Cyberspace*, SWP-Studie 18/2014 (Berlin: Stiftung Wissenschaft und Politik, October 2014), 25. Article 28ff of the draft articles of the United Nations International Law Commission on the responsibility of states: International Law Commission, "Responsibility of States for Internationally Wrongful Acts", in *Yearbook of the International Law Commission*, vol. II, part 2 (New York and Geneva, 2001): 26–143; also published as an annex to United Nations General Assembly, *Responsibility of States for Internationally Wrongful Acts*, Resolution 56/83 (New York, 12 December 2001).

12 United Nations General Assembly, *Combating the Criminal Misuse of Information Technologies*, Resolution 55/63 (New York, 4 December 2000), http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf (accessed 30 November 2015).

13 United Nations General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174 (New York, June 2015).

14 For the international law of the Web, see Schaller, *Internationale Sicherheit und Völkerrecht im Cyberspace* (see note 11).

15 The collaboration of IT emergency teams (Computer Emergency Response Team, CERT) in the CyberGreen project (www.cybergreen.net) could serve as a model. Here, CERTs from the Pacific Region states as well as Japan and China work together to ensure a "green cyberspace".They perceive themselves as strictly technical, but the project is nevertheless based on the idea of jointly identifying and rectifying weak areas, such as malware or vulnerable networks.

16 An example is the debate about communications encryption and the divergent positions of the security agencies on the one hand and industry representatives on the other hand. On this point, see also Berklett Cybersecurity Project, ed., *Don't Panic: Making Progress on the "Going Dark" Debate* (Cambridge, MA: Berkman Center for Internet and Society at Harvard, February 2016).

17 These vital requirements derive from the results of the 2015 SWP CyberLabs (see note 3).

18 On the concept of responsibility in international relations, see the results of the conference on "Politik und Verantwortung" (Frankfurt/Main, 10–12 February 2016), to be published in 2017 in a special issue of the *Politische Vierteljahresschrift* (PVS). See also Christopher Daase and Julian Junk, eds., *Internationale Schutzverantwortung – Normative Erwartungen und politische Praxis*, Sonderheft der *Friedens-Warte* 88, no. 1–2 (2013); Hanns W. Maull, "What German Responsibility Means", *Security and Human Rights* 26, no. 1 (2015): 11–24.

substantial parts of the minority. Especially in times of crisis, the so-called rallying effect is an indispensable element of democratic resilience."[19] However, the inclusiveness of legislative processes should stop wherever private-sector actors start exerting a dominant influence on legislative bodies.[20] This can only be countered with transparent and representative processes that also give other states a minimum of certainty that their legitimate interests are being taken into consideration. The openness of a political system is, in turn, a fundamental prerequisite for states trusting one another so that they can deliver their individual contributions to producing the public good of a "secure cyberspace". These requirements are far from easy to meet. In a technically challenging area such as international cyber policy and cybersecurity policy, consultations often need to be confidential. Furthermore, the expertise of large companies almost inevitably dominates this field, making it extraordinarily difficult for civil-society representatives or members of parliament to be accepted as competent interlocutors. Special efforts are therefore required to prevent one-sided representations of interests or the instrumentalisation of policy by the industry.[21]

A maxim of Germany's self-perception in foreign policy states that regulatory practices should be coordinated as closely as possible with its most important European partners.[22] The internal market is so tightly interconnected through digital technologies – as indeed are its foreign and security policies – that individual member states' policies in cyberspace are ineffective in comparison to a regional European approach.

- Through its international cyber policy, Germany intends to achieve effective collaboration on cybersecurity in Europe and across the world. German measures to promote a free and secure Internet should therefore always be integrated at the European or transatlantic level. No state can seriously claim to be able to regulate cyberspace on its own. Germany will only be able to gain sufficient negotiating power on the global stage if it coordinates intensively with the leading European cybernations (France, Great Britain, Netherlands, Sweden, Italy, Spain and Poland) and if it uses EU structures such as the Friends of the Presidency Group on Cyber Issues (FoP Cyber).[23] Only regulatory processes coordinated at the European level can prevent globalisation and digitalisation from aggravating the symptoms of the crisis in European integration.

For historical reasons, it is self-evident for Germany that the militarisation and securitisation of cyberspace[24] must be counteracted. Due diligence also signifies that states should not merely orientate themselves along national interests, but also think in the categories of global public good. Germany's tradition of civilian power[25] is perpetuated in its international cyber policy and cybersecurity policy as well.

- The German Federal Republic has always held to the principle of generally pursuing its interests through economic and political rather than military means. In view of this tradition, the only responsible international cyber policy and cybersecurity policy is one that tries to civilise international policy in cyberspace. That would mean internationalising socially accepted norms as much as possible – for example in the GGE, OSCE and

19 Christopher Daase, "Innenpolitische Voraussetzungen erfolgreicher Cyber-Außen- und Sicherheitspolitik", lecture given at the CyberLab of the Stiftung Wissenschaft und Politik (SWP) (Berlin, 8 September 2015). A "rallying-effect" is a short-term but far-reaching and broad public agreement with or toleration of exceptional measures, especially in times of crisis.

20 For example, lobbying by the industry during the drafting of the new EU General Data Protection Regulation (GDPR) culminated in entire passages of text from trade-association position papers being reproduced in the amendments to the legislative act. Patrick Beuth, "Bundesregierung hofiert Lobbyisten", *Zeit Online*, 10 March 2015, http://www.zeit.de/digital/datenschutz/2015-03/eu-datenschutzgrundverordnung-ministerrat-bundesregierung-lobbyplag (accessed 30 November 2015).

21 Liz Alderman, "Terror Threats Thaw Budgets across Europe", *New York Times*, 31 January 2016.

22 Recommended reading on Germany's self-perception in foreign policy is Gunther Hellmann, "Germany's World: Power and Followership in a Crisis-Ridden Europa", *Global Affairs* 2, no. 1 (2016): 3–20.

23 The FoP Cyber was created in 2013 for a three-year period as a permanent body to monitor the implementation of Europe's cyberstrategy. The group has evolved into the most important EU forum for discussing and following up on all cybertopics.

24 On this point, see inter alia Ronald J. Deibert, *Black Code: Inside the Battle for Cyberspace* (Toronto: McClelland & Stewart, 2013); Myriam Dunn Cavelty, *Cybersecurity and Threat Politics: US Efforts to Secure the Information Age* (London: Routledge, 2008); Myriam Dunn Cavelty, "Cybersecurity and the Negative Consequences of State Action", paper given at the conference "The Future of International Order", at the Stiftung Wissenschaft und Politik, Berlin, 29 November – 1 December 2015.

25 Knut Kirste and Hanns W. Maull, "Zivilmacht und Rollentheorie", *Zeitschrift für Internationale Beziehungen* 3, no. 2 (1996): 283–312; Maull, "What German Responsibility Means" (see note 18).

other governmental organisations and fora – and thereby repressing the violent assertion of regulations. Military violence – including an active cyberdefence[26] based on deterrence – could only be justified at the national level in cases of self-defence and where it was coordinated with the EU and Nato member states on the one hand and was decided by the German Parliament. Responding to cyber attacks with automatic counterattacks and digital acts of reprisal would be extremely problematic. For one thing, any attempt to attribute cyber attacks unequivocally raises all sorts of technical, legal and political questions; for another, counterattacks can have serious side-effects. Active cyberdefence might provoke a digital arms race – for instance through Advanced Persistent Threats (APTs[27]) – with incalculable risks for fragile critical infrastructure. From a due diligence perspective, a strategy of "deterrence-by-resilience"[28] is therefore preferable. With their new IT-security law and the NIS (Network and Information Security) directive, Germany and the EU are leading by example in creating resilient information and communications structures in critical infrastructure and in setting minimum standards in IT security. Research into resilience, prevention, peace and conflict has a key role to play in cybersecurity when it comes to civilising politics.

In due diligence, material and procedural contents merge into an overarching norm. For the purposes of due diligence, cybersecurity also comprises a certain form of political regulation. This is about "resist[ing] the securitisation of the Internet and of Internet policy. The goal should not so much be security in abstracto as resilience, meaning the ability to withstand shocks. And that can only be achieved through complex structures involving the whole of society".[29] An international cyber policy and cybersecurity policy is based on a broad understanding of security and involves all stakeholders such as the state, academia, industry and society.[30]

26 Offensive strategies aim at "attacking the systems of other states, sabotaging them, gaining control over them, rendering them inoperative or causing malfunctioning". But it is a matter of "securing and sustaining one's own IT structures and communications and weapons systems, and protecting them against being influenced or attacked, by using so-called defensive approaches." German Parliament, *Kleine Anfrage der Abgeordneten Dr. Alexander Neu u.a.: Krieg im "Cyber-Raum" – offensive und defensive Cyberstrategie des Bundesministeriums der Verteidigung*, Drucksache 18/6496 (Berlin, 16 October 2015). On this classification, see also Robert S. Dewar, *The "Triptych of Cybersecurity": A Classification of Active Cyber Defence*, contribution to the 6th International Conference on Cyber Conflict, Tallinn, 3–6 June 2014.

27 APTs occur in waves. After infiltrating a system, the malware remains hidden and accesses data in stages. Without effective protective tools, it can take weeks or even months just to discover the security breaches and attacks. See German Federal Office for Information Security, *Die Lage der IT-Sicherheit in Deutschland 2015* (Bonn, November 2015), 26f.

28 Michael Rühle, "Das Prinzip Abschreckung", *Frankfurter Allgemeine Zeitung*, 31 March 2015. See also Annegret Bendiek and Tobias Metzger, *Deterrence Theory in the Cyber-Century*, Berlin: Stiftung Wissenschaft und Politik, May 2015 (SWP EU/Europe Division Working Paper 2/2015).

29 Daase, "Innenpolitische Voraussetzungen erfolgreicher Cyber-Außen- und Sicherheitspolitik" (see note 19).

30 The multi-stakeholder model was laid down as the foundation for Internet Governance at the World Summit on the Information Society (WSIS II) in Tunis in 2005. During the UN Summit held in December 2015 as part of the WSIS follow-up process, there was disagreement on how this model, which has been successfully used in the Internet Governance Forum (IGF) and the Internet Corporation for Assigned Names and Numbers (ICANN), might be developed further.

Due Diligence in Institutional Practice

German policies are already beginning to take due diligence into account to some extent, but the norm is not yet sufficiently embedded in German institutions. From this perspective, the coherence and the consistency of content of Germany's international cyber policy and cybersecurity policy must be closely scrutinised. Its current institutional structure reflects the fact that the implementation of due diligence has already come a long way. The responsible authorities are now closely interconnected. However, it is also clear that much still needs to be improved with a view to European cooperation, inclusiveness and civilian response.

Institutional Structures

The German Federal Government has committed to creating a complete instrumentarium in coordination with the responsible state authorities to defend against cyber attacks.[31] This is intended to contribute to guaranteeing security provisions for the state as a whole. The development of fully differentiated responsibilities is politically willed.[32] Germany's international cyber policy and cybersecurity policy contains a whole series of cooperations, which essentially rest on five pillars.

First Pillar: The Federal Office for Information Security
In Germany, overall ministerial control over cybersecurity issues rests with the German Federal Ministry of the Interior (BMI).[33] The Federal Office for Information Security (BSI) is the Federal Government's most important service provider in IT security. It reports to the BMI. The BSI is also responsible for operations to repel attacks against the Federal Government's IT infrastructure. It has an IT emergency team (CERT-Bund) at its disposal for this. The Federal Office fulfils its mission as "the central reporting office for security in Federal-Government IT", in charge of "repelling harmful programmes and threats to the Federal Government's communications technology", "stipulating guidelines on security standards" and providing certifications.[34] Because of the high quality of the BSI standard (ISO 27001) for promoting certified basic functions, and because of other recommendations, the BSI enjoys a high level of European and international recognition. For years, it has been involved in an intensive international exchange of experience and information at the management and professional levels. At the operations level, cooperation with other IT emergency teams is especially important. CERT-Bund belongs to the interdisciplinary International Watch and Warning Network (IWWN).[35] At the domestic level, the BSI initiated the founding of the Allianz für Cybersicherheit (alliance for cybersecurity), which now pools German know-how on cybersecurity and has become the main point of contact for companies and citizens.[36] The Federal Office of Bundeswehr Equipment, Information Technology and In-Service Support (BAAINBw) and the IT emergency team of the German armed forces (CERTBw) work closely with the BSI, in particular with its IT situation and analysis centre and the CERT-Bund team.

Second Pillar: The National Cyberdefence Centre
A vital step towards implementing due diligence was taken in 2011 with the creation of the National Cyberdefence Centre.[37] This information platform is intended

31 German Federal Ministry of the Interior, ed., *Cyber-Sicherheitsstrategie für Deutschland* (see note 4).
32 In Norway, for instance, the national cybersecurity strategy is part of the portfolio of the ministry of justice. The Norwegian Ministry for Foreign Affairs is currently elaborating a Global Strategy for Cyberspace.
33 German Federal Ministry of Defence, *Weißbuch 2016*, http://www.bmvg.de/portal/a/bmvg/!ut/p/c4/04_SB8K8xLLM9MSSzPy8xBz9CP3I5EyrpHK9pNyydL3y1Mzi4qTS5Az9gmxHRQBg2ftX/ (accessed 30 November 2015).
34 German Federal Ministry of Justice and Consumer Protection, ed., *Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG)*, last modified on 17 July 2015, http://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html (accessed 30 November 2015).
35 IT Law Wiki, *International Watch and Warning Network*, http://itlaw.wikia.com/wiki/International_Watch_and Warning_Network (accessed 30 November 2015).
36 German Federal Office for Information Security, *Allianz für Cyber-Sicherheit*, http://www.allianz-fuer-cybersicherheit.de/ACS/DE/Home/startseite.html (accessed 30 November 2015).
37 The Centre groups together representatives of the BSI, German Federal Office of Civil Protection and Disaster Assistance

to simplify cooperation between the various government agencies and improve measures to protect against and repel IT attacks. The Centre is also part of the state's project-based collaboration with companies and service providers, and with foreign security services. The separation rule is a fundamental tenet of German federal legislation and stipulates that the tasks of the police and the intelligence services must be carried out by different, organisationally distinct authorities. Counter-intelligence is the purview of the BfV while the BKA is responsible for policing criminally motivated IT attacks. The technical information department (TA) of the Federal Intelligence Services (BND) retrieves information by technical means (Signals Intelligence or SIGINT); it obtains, in accordance with its official mandate, information that is significant for Germany's foreign and security policy; and it evaluates it.[38] Using this information, the BND also supports the German armed forces in their cyberdefence.

Third Pillar: The National Cybersecurity Council

When dealing with the challenges of cybersecurity, strong coordination with the state as a whole must be ensured.[39] To this end, the interministerial National Cybersecurity Council, chaired by the Federal Commissioner for Information Technology, brings together the secretaries of state.[40] Furthermore, in Germany, IT security is a federal issue. The Cybersecurity Council consists of two federal-state representatives, representatives of several federal authorities – the BKA; the Federal Ministry for Foreign Affairs (AA); the Federal Ministries of the Interior; of Education and Research; of Defence (BMVg); for Economic Affairs and Energy (BMWi); of Justice and Consumer Protection; and of Finance – as well as four associated bodies representing the industry (the Federation for the Information Economy, Telecommunications and New Media; the Federation of German Industries; the Association of German Chambers of Commerce and Industry; and the transmission system operator Amprion GmbH). Since 2013, the Cybersecurity Council has been meeting three times a year. Fundamental issues of federal IT management and security are also dealt with in the interministerial council of IT commissioners (also called the IT Council).

Fourth Pillar: An International Cyber Policy

Germany's 2011 cybersecurity strategy stipulates the development of a targeted and coordinated international cyber policy that makes it possible to take preventative measures for IT security in Germany, particularly to protect critical infrastructure and for international cooperation.[41] This international cyber policy includes a representation of German interests with the EU and other international organisations and bodies, and in bilateral dialogues. In 2011, the Ministry of Foreign Affairs created its coordination staff for international cyber policy.[42] This staff serves as the interface between national ministerial policies on the one hand and the effort to coordinate the international exertion of influence on the other hand, with the aim of creating a climate of security and trust, such as is indispensable for a defensive cybersecurity strategy.

Fifth Pillar: The German Armed Forces

Measures taken by the German military should be limited to protecting their own capacity to act in accordance with their mandate, "so as to embed cybersecurity as a part of the security provisions for the state as a whole".[43] This is the responsibility of the German mili-

(BBK), domestic intelligence service (BfV), German Intelligence Services (BND), Federal Criminal Police Office (BKA), Customs Investigation Bureau (ZKA), Federal Police (BPol) and Armed Forces. Federal Ministry of the Interior, *Nationales Cyber-Abwehrzentrum*, http://www.bmi.bund.de/DE/Themen/Sicherheit/IT-Cybersicherheit/Cyberabwehrzentrum/cyberabwehrzentrum_node.html (accessed 22 February 2016).

38 According to media reports, in 2014 the Federal Parliament's budget committee made 300 million euros available to the BND for implementing the so-called Strategic Technology Initiative (SIT), a technological modernisation programme.This total, to be paid in yearly tranches until 2020, is intended to expand the technical capabilities of the BND. John Goetz and Hans Leyendecker, "Aufrüsten für den Cyberkampf", *Süddeutsche Zeitung*, 10 November 2014, http://www.sueddeutsche.de/digital/bundesnachrichtendienst-aufruesten-fuer-den-cyberkampf-1.2211761 (accessed 5 February 2016).

39 Carsten Köppl, *IT-Sicherheit föderalisiert sich*, summary of the "Public IT-Security" (PITS) conference (Berlin, 25/26 September 2013), http://www.public-it-security.de/icc/public/nav/e86/e862fd19-3c66-6413-ccca-2a307b988f2e.htm.

40 German Federal Ministry of the Interior, *Cyber-Sicherheitsrat*, http://www.bmi.bund.de/DE/Themen/Sicherheit/IT-Cybersicherheit/Cybersicherheitsrat/cybersicherheitsrat_node.html (accessed 22 February 2016).

41 Federal Ministry of the Interior, ed., *Cyber-Sicherheitsstrategie für Deutschland* (see note 4).

42 Federal Ministry of Foreign Affairs, *Cyber-Außenpolitik*, http://www.auswaertiges-amt.de/DE/Aussenpolitik/GlobaleFragen/Cyber-Aussenpolitik/KS_Cyber-Aussenpolitik_node.html (accessed 5 February 2016).

43 Federal Ministry of the Interior, ed., *Cyber-Sicherheitsstrategie für Deutschland* (see note 4).

tary's CNO forces,[44] which are to be expanded further and to be used for active cyberdefence in future.[45] This seems to indicate a potential paradigm change from defensive to offensive cyberprotection. In September 2015, German Defence Minister Ursula von der Leyen confirmed that "a new goal is being developed for cyberspace and IT, both downstream and in the ministry".[46] The creation of a pool of IT reservists is planned for specific military cyber operations. There are also plans for giving Military Counter-Intelligence (MAD) an expanded counter-intelligence mission for deployment abroad, to cover all persons who might pose a risk to the armed forces' security or readiness for duty.[47] Acording to Colonel Joachim Smola, permanent representative of the MAD president, the MAD is "much more [...] than a purely defensive intelligence service", but rather a "comprehensive service provider on security issues, and it advises and supports the German armed forces [...] both at their garrisons and on foreign deployment".[48]

At the parliamentary level, currently three main bodies control fundamental areas of the cybersecurity strategy that concerns the Federal Government's intelligence activities: the parliamentary oversight committee (PKGr), G-10 Committee and the NSA committee of inquiry. The panels of experts – the digital-agenda committee, interior committee, foreign committee, defence committee – handle further topics of the international cybersecurity policy. Cyberspace makes no distinction between domestic and foreign policy. Parliament, in its work to uphold democracy and the rule of law, must take this insight into account both conceptually and institutionally. Domestic policy should be adjusted in accordance with due diligence. This is the only way of restoring the citizens', allies' and EU partners' trust lost during the Edward Snowden leaks. Trust is an indispensable prerequisite for European cooperation and politics. However, the implementation of the three major challenges to an international cyber policy and cybersecurity policy – namely Europeen cooperation, inclusiveness and civilian response – still leaves much to be desired:

European Cooperation

The methods used at the federal and EU levels to establish an overview of the cyber threat situation are unsatisfactory. To render criminal prosecutions more successful, proposals have been put forward to transform the National Cyberdefence Centre into an umbrella body for IT security (comparable to the Joint Anti-Terrorism Centre), since it does not currently bring together all federal and state authorities. There are also calls for more cooperation between national and EU authorities with a view to a European exchange of information.[49] Some important partners, such as France or the Netherlands, criticise Germany not only because they find the "German position" frequently unclear, but also because they do not always know with which ministry to negotiate as part of the European coordination. Moreover, vital coordination at the EU level is sluggish, inter alia because the attribution of specific responsibilities is so complicated. Since the parliamentary elections of 2013, coalition partners have been discussing whether Germany needs an Internet ministry or a so-called digital agency.[50] However, they have only been able to agree on an office without power or resources: the office of Digital Champion of the Federal Government, currently held by Gesche Joost.

44 Computer Network Operations (CNO) are non-kinetic means of attack, which work by implementing computer codes or computer programmes in cyberspace. They serve to manipulate, disrupt or even destroy enemy information and communications systems as well as protect states' own systems or gather information from data sources that are not publicly available. CNOs are therefore subdivided into Computer Network Attacks (CNA), Computer Network Defence (CND) and Computer Network Exploitation (CNE).

45 Federal Ministry of Defence, "Tagesbefehl der Ministerin: Bundeswehr wird im Cyber-Raum zukunftsfähig" (Berlin, 17 September 2015).

46 Ibid.

47 Andre Meister, "Geheime Cyber-Leitlinie: Verteidigungsministerium erlaubt Bundeswehr 'Cyberwar' und offensive digitale Angriffe", *netzpolitik.org*, 30 July 2015, https://netzpolitik.org/2015/geheime-cyber-leitlinie-verteidigungsministerium-erlaubt-bundeswehr-cyberwar-und-offensive-digitale-angriffe/ (accessed 30 November 2015).

48 "Geheimhaltung versus Transparenz", *Behörden Spiegel* (November 2015): 48.

49 Since 2011, the European External Action Service has been responsible for the EU Intelligence Analysis Centre (EU INTCEN), which produces civilian situation analyses for EU decision-makers based on material delivered by national intelligence services. European External Action Service, *EUINTCEN Fact Sheet* (Brussels, 5 February 2015), http://eeas.europa.eu/factsheets/docs/20150206_factsheet_eu_intcen _en.pdf (accessed 5 February 2016).

50 German Federal Ministry for Economic Affairs and Energy, *Digitale Strategie 2025* (Berlin, March 2016).

Inclusiveness

Downstream authorities such as the BSI, BKA or BND have already fundamentally adapted their institutions to repelling cyber attacks. In part, these reforms have only become public knowledge through leaked documents.[51] However, the BSI's much-discussed institutional dependency remains unchanged.[52] In February 2016, the German Federal Cabinet appointed the president of the Cybersecurity Council, Arne Schönbohm, to be the president of the BSI. The public views his links to the IT and arms industries with suspicion. Critics also point out "that there are six to ten times the resources available for the offensive approach than there are for the defensive approach to cyber attacks or compromised IT security".[53] Besides, according to a member of the executive board of the Federal Association of the Information Economy, Telecommunications and New Media (Bitkom), Susanne Dehmel, only one in five companies makes use of the IT consultancies offered by the government.[54] Moreover, companies that have fallen victim to cyber attacks tend to contact their state's agency for internal security rather than the police, since the latter would have to launch a preliminary investigation wherever a criminal act was suspected. Consultations are underway on reforming the intelligence services as well as improving parliamentary oversight of those services by the PKGr.[55]

While the special rapporteur appointed by the Federal Government, Kurt Graulich, did examine the so-called NSA selector lists, which had been passed to the BND, the results leave many questions unanswered. In 2015, the former president of the BfV and BND, Hansjörg Geier, argued that a code needed to be elaborated for regulating the exchange of information by intelligence services and that a post of parliamentary ombudsperson for the intelligence services needed to be created, modelled on the parliamentary ombudsperson for the armed forces.[56]

Civilian Response

The permanent secretary to the Federal Ministry of the Interior, Hans-Georg Engelke, who is also the Federal Government's IT Commissioner, emphasised that it was vital for the authorities to cooperate on IT security, but that the BMI had overall control on issues of cybersecurity. However, this claim is already being questioned as part of the 2016 white-paper discussion. Even the National Cybersecurity Council has not been able to solve the problem of the at-times inefficient distribution of resposibilities. In July 2013, while elucidating the NSA affair, the German Federal Government did publish an eight-point programme on improving protection of the private sphere.[57] However, the Cybersecurity Council did not publicly take a position on the questionable practices of the security services – for instance, committing industrial espionage[58] or keeping selector lists with spying targets.[59]

51 Following the leaks, Chief Federal Prosecutor Harald Range launched preliminary proceedings against the Internet portal *netzpolitik.org,* on suspicion of treason. However, the case was dropped after political intervention. See "Maas zweifelt an Verfahren gegen 'netzpolitik.org'", *Zeit Online*, 31 July 2015, http://www.zeit.de/digital/internet/2015-07/netzpolitik-ermittlungen-journalisten-innenministerium-maassen (accessed 30 November 2015).

52 Despite media claims to the contrary – see e.g. "Bundesamt für Sicherheit in der Informationstechnik (BSI) soll neue Bundesbehörde werden", *Der Spiegel*, 10 August 2014 – the BSI continues to report to the BMI. See *Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG), § 1 Bundesamt für Sicherheit in der Informationstechnik*.

53 Ingo Ruhmann, "Aufrüstung im Cyberspace. Staatliche Hacker und zivile IT-Sicherheit im Ungleichgewicht", *Kriegführung im Cyberspace*, supplement to *Wissenschaft und Frieden*, no. 3 (2015): 12–16 (Dossier 79).

54 German Federal Ministry of Defence, "Weißbuchprozess: Bundeswehr sucht Dialog mit Cyber-Community" (Berlin, 18 September 2015).

55 Thomas Oppermann, Christian Flisek and Burkhard Lischka, *Rechtsstaat wahren – Sicherheit gewährleisten!* (Berlin: SPD-Bundestagsfraktion, 16 June 2015), http://www.spdfraktion.de/sites/default/files/2015-06-16-eckpunkte_reform_strafma-r-endfassung.pdf (accessed 30 November 2015).

56 Rudi Wais, "So könnte eine bessere Kontrolle der Nachrichtendienste aussehen", *Augsburger Allgemeine*, 3 May 2015, http://www.augsburger-allgemeine.de/politik/So-koennte-eine-bessere-Kontrolle-der-Nachrichtendienste-aussehen-id33933952.html (accessed 30 November 2015).

57 Federal Ministry of Defence/Federal Ministry of Industry and Technology, *Maßnahmen für einen besseren Schutz der Privatsphäre*, Fortschrittsbericht (Berlin, 14 August 2013), http://www.bmi.bund.de/SharedDocs/Downloads/DE/Nachrichten/Pressemitteilungen/2013/08/bericht.pdf?__blob=publicationFile.

58 German Federal Parliament, *Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Jan Korte, Dr. André Hahn, Ulla Jelpke, weiterer Abgeordneter und der Fraktion Die Linke. Geheimdienstliche Angriffe und Spionage bei deutschen Unternehmen*, Drucksache 18/2281 (Berlin, 5 August 2014).

59 German Federal Parliament, *Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion der SPD. Abhörprogramme der USA und Umfang der Kooperation der deutschen Nachrichtendienste mit den US-Nachrichtendiensten*, Drucksache 17/14560 (Berlin, 14 August 2013); German Federal Parliament, *Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Jan Korte, Christine Buchholz, Ulla*

Nor did it comment on the cyber attack on the German parliament. Many observers had expected a more proportionate reaction to the attack on Germany's highest constitutional body.

Digital Industrial Policy and the Importance of Private Actors

Due diligence requires not only that institutional structures be constructed, it also needs sophisticated capabilities in information and communications technology (ICT) and their "intelligent connectivity".[60] Over the past few decades, automisation has allowed the German economy to respond well to the global pressures to be competitive and innovative. The Federal Ministry for Economic Affairs wants to further boost small and medium enterprises using its Digital Strategy 2025. Private actors play an extraordinarily important role in the Federal Government's international cybersecurity policy. Industrial locations gain in strategic importance. The companies located there not only create jobs and added value, but also set competitivity standards for whole economies.[61] The German Federal Government believes that there is still plenty of untapped potential in Germany's ICT: according to a study by the Fraunhofer Institute for Systems and Innovation Research, Intelligent Networks could generate overall benefits to German society worth 56 million euros a year.[62]

However, other countries have digitalised more successfully. The pioneering companies are mostly American, South Korean and Chinese. In 2014, the German Federal Government launched the programmes Digital Agenda and Digital Management. However, these programmes are meagrely equipped compared with the US government's programmes for funding research projects, for instance on developing quantum computers or the capability of analysing big-data. The future project Industrie 4.0 has federal funding to the tune of around 200 million euros from the BMBF and BMWI. That is still not nearly enough to make them competitive. It must be remembered that, to meet due diligence requirements, the digital industrial policy curently being developed needs the public and private sectors to cooperate, needs to be integrated into European harmonisation and needs to focus on a defensive cybersecurity policy.

European Cooperation

There has been criticism from the academia that "the Industrie 4.0 discourse [is] often too technical and national",[63] and that it needed to be more closely interconnected at the EU level than hitherto, because where (critical) infrastructure was concerned, solutions for data security, operational safety and data protection were not being brought together.[64] This is also reflected in the Federal Government's programme Digital Agenda 2014–2017. It outlines seven fields of action including the "European and international dimension".[65] According to the CDU, CSU and SPD coalition agreement, a "European space of trust" is supposed to be created,[66] but primarily with the help of national "measures to regain technological sovereignty".[67] It is not communicated by the government how this obvious contradiction could be resolved. National IT summits are dominated by interested parties

Jelpke, weiterer Abgeordneter und der Fraktion Die Linke. Aktivitäten der Bundesregierung zur Aufklärung der NSA-Ausspähmaßnahmen und zum Schutz der Grundrechte, Drucksache 18/159 (Berlin, 12 December 2013); German Federal Parliament, *Hitzige Debatte über die BND-NSA-Kooperation* (Berlin, 21 May 2015), http://www.bundestag.de/dokumente/textarchiv/2015/kw21_de_aktuelle_stunde_nsa/375278 (accessed 5 February 2016).

60 German Federal Parliament, *Unterrichtung durch die Bundesregierung. Strategie Intelligente Vernetzung*, Drucksache 18/6022 (Berlin, 18 September 2015), http://dip21.bundestag.de/dip21/btd/18/060/1806022.pdf (accessed 30 November 2015).

61 Initiative D21, ed., *D21-Digital-Index 2015. Die Gesellschaft in der digitalen Transformation* (Berlin, 2015).

62 German Federal Parliament, *IKT-Potenziale nicht ausgeschöpft* (Berlin, 2 October 2015), http://www.bundestag.de/presse/hib/2015_10/-/390352 (accessed 30 November 2015).

63 Sabine Pfeiffer, "Industrie 4.0 und die Digitalisierung der Produktion – Hype oder Megatrend?", *Aus Politik und Zeitgeschichte* 65, no. 31–32 (2015): 6–12.

64 According to Peter Liggesmeyer, director of the Fraunhofer Institute for Experimental Software Engineering and president of the German Informatics Society, speaking to the Digital Agenda committee; see "Umfassende Sicherheit für Industrie 4.0", *heute im bundestag*, no. 345 (1 July 2015).

65 German Federal Ministry for Economic Affairs and Energy/German Federal Ministry for Traffic and Digital Infrastructure, ed., *Digitale Agenda 2014–2017* (Berlin, August 2014), http://www.digitale-agenda.de/Content/DE/_Anlagen/2014/08/2014-08-20-digitale-agenda.pdf?__blob=publication File&v=6 (accessed 30 November 2015).

66 *Deutschlands Zukunft gestalten. Koalitionsvertrag zwischen CDU, CSU und SPD. 18. Legislaturperiode* (Berlin, 27 November 2013), http://www.bundesregierung.de/Content/DE/_Anlagen/2013/2013-12-17-koalitionsvertrag.pdf?__blob=publicationFile (accessed 30 November 2015).

67 Ibid., 147.

backed by well-organised, well-funded actors with a wide range of competences. Their special focus is first and foremost the German industrial policy. However, Industrie 4.0, meaning the Internet of Things, can only be designed at the European or even global level.[68]

In May 2015, the European Commission presented a strategy for the digital single market.[69] It expects this market, once realised, to contribute 520 billion euros to EU states' gross domestic product. However, the Commission currently has only limited means available for developing key digital technologies. The Connecting Europe Facility (CEF) has budgeted about a billion euros spread over seven years for ICT funding for the EU member states. The financing programme Horizon 2020 is making 7.2 billion euros available for research for the EU 28, from 2014–2020.[70] Since the Juncker Commission took up its posts in November 2014, the Industrie 4.0 policy has been developed into a digital single market at the EU level with the help of a comprehensive legal package. In the Commission's view, policies to create and regulate the market, as well as distributive policies should be got off the ground as quickly as possible. Attaining the necessary speed is a problem, however, because the Commission first has to harmonise the legal policies of all 28 member states. A number of leading decisions published by the European Court of Justice (ECJ) in 2014 and 2015 are seen as important milestones of a European or transatlantic agreement on data-security and data protection policy.Important decisions in this context are those on the illegality of telecommunications data retention, on the right to be forgotten and on the illegality of the Safe Harbour Agreement.[71] Even the legal status of its successor agreement between the EU and the US, the Privacy Shield, continues to be disputed.[72] Furthermore, in late December 2015, the European Parliament, Council and Commission agreed a General Data Protection Regulation and a directive on network and information security.[73] Industry representatives, however, view European harmonisation more critically. They consider the ECJ decisions and the Commission's legal initiatives to be "using politics for a digital industrial policy"[74] and to be protectionist.

Inclusiveness

The importance of private actors can also be seen in the fact that they run much critical infrastructure, such as hospitals, banks, energy concerns and waterworks. Additionally, private actors often have the relevant knowledge for gauging threat levels and developing tools to defend against threats. Only banks know how often they are attacked, and without information from industrial companies about espionage, no intelligence service can take meaningful countermeasures. Every act of regulation, development of standards and formulation of policy should therefore be carried out in solidarity with the private sector, if possible through public-private partnerships (PPP). For

68 German Parliament, *Antrag der Fraktionen der CDU/CSU und SPD, Industrie 4.0 und Smart Services – Wirtschafts-, arbeits-, bildungs- und forschungspolitische Maßnahmen für die Digitalisierung und intelligente Vernetzung von Produktions- und Wertschöpfungsketten*, Drucksache 18/6643 (Berlin, 10 November 2015), 3; Ansgar Baums, Martin Schössler and Ben Scott, eds., *Kompendium Industrie 4.0. Wie digitale Plattformen die Wirtschaft verändern – und wie die Politik gestalten kann* (Berlin, October 2015).

69 European Commission, *A Digital Single Market Strategy for Europe*, COM(2015) 192 final (Brussels, 6 May 2015), http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52015DC0192&from=IT (accessed 30 November 2015).

70 European Commission, *Horizon 2020. The EU Framework Programme for Research and Innovation*, https://ec.europa.eu/programmes/horizon2020/ (accessed 30 November 2015); Eric Maurice, "China to Join Juncker's Investment Scheme", *EU Observer* (28 September 2015).

71 European Court of Justice, *Judgment of the Court: "*Electronic communications – Directive 2006/24/EC – Publicly available electronic communications services or public communications networks services – Retention of data generated or processed in connection with the provision of such services – Validity – Articles 7, 8 and 11 of the Charter of Fundamental Rights of the European Union)" (Luxembourg, 8 April 2014), http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN (accessed 30 November 2015); European Court of Justice, "An Internet search engine operator is responsible for for the processing that it carries out of personal data which appear on web pages published by third parties", press release no. 70/14 (Luxembourg, 13 May 2014); European Court of Justice, "The Court of Justice declares that the Commission's US Safe Harbour decision is invalid", press release no. 117/15 (Luxembourg, 6 October 2015).

72 Annegret Bendiek and Evita Schmieg, *EU-Außenhandel und Datenschutz. Wie lässt sich beides besser vereinbaren?*, SWP-Aktuell 10/2016 (Berlin: Stiftung Wissenschaft und Politik, February 2016).

73 European Parliament, *Personal Data Protection: Processing and Free Movement of Data (General Data Protection Regulation)*, Procedure File 2012/0011(COD), http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2012/0011 (accessed 30 November 2015).

74 Ansgar Baums, "Der weiße Elefant: Industriepolitik durch die Hintertür des Datenschutzes?", *plattform-maerkte.de*, 10 March 2015, http://plattform-maerkte.de/der-weisse-elefant-industriepolitik-durch-die-hintertuer-des-datenschutzes/ (accessed 30 November 2015).

example, Germany introduced measures to protect critical infrastructure in 2007 through the UP KRITIS, a PPP of operators of such infrastructure.[75] At the EU level, the Commission presented a draft directive for network and information security in 2013. The directive is intended to make IT more secure for operators of critical infrastructure and large online service providers, and will oblige affected companies to report any security and data protection events or IT attacks. These requirements are intended for all operators and providers of "essential services", such as in energy, water supply, transport, finance, health and the Internet. The draft lists Internet exchanges, domain registration sites, online marketplaces and search engines, but not social networks. Small digital companies are also excluded. According to the directive, member states will have to build national reporting systems and exchange information with each other. "Competent authorities" such as the BSI, as well as specific Computer Security Incident Response Teams (CSIRTs) in addition to the already existing CERTs will be involved. The German Federal Government used the long negotiation period from 2013 to 2015 to reach a solution nationally with its industry, before the EU agreed on the topic. The German Parliament passed its IT security law in July 2015, and thus introduced reporting obligations for serious cyber attacks and minimum standards for protecting critical infrastructure earlier than the EU.[76]

However, close cooperation between state authorities and private companies working in the area of critical-infrastructure security is not without risks. It is especially questionable whether the private sector can self-regulate if state actors allow themselves to become dependent on the interests of individual private actors to the point where they are barely able to act meaningfully without them.[77] This dependency becomes the more dangerous, the more tightly these companies monopolise the relevant knowledge. In such cases, the state must be careful to ensure that members of parliament and civil-society representatives regularly get the opportunity for critical questioning and for being involved in consulting processes.[78] It is part of due diligence that not only the national and EU decisions but also the preparatory processes for decision-taking remain inclusive and open to the concerns of civil society, small and medium enterprises, and independent scholarship.

Civilian Response

Governments must resist the temptation to react to the growing number of digital attacks by building a digital arms industry and offensive cyberweapons.[79] The defence policy guidelines issued by the German Federal Ministry of Defence in May 2011 already contain the stipulation that the German armed forces must encompass a range of abilities that is as broad as possible.[80] Militarily, cyberspace is categorised as a so-called operative domain, comparable to land, air, ocean or space. According to the April 2015 Strategic Guideline on Cyberdefence, the military should be able "to limit, and if necessary even switch off, opponents' use of the Internet and mobile communications" during operational missions.[81] Such formulations and strategic decisions carry the risk of securitising or even militarising cyberspace, and thus creating a new threat scenario.[82] This is conspicuous at conferences

75 UP KRITIS office, ed., *UP KRITIS. Öffentlich-Private Partnerschaft zum Schutz Kritischer Infrastrukturen* (Bonn, February 2014), http://www.kritis.bund.de/SharedDocs/Downloads/Kritis/DE/UP_KRITIS_Fortschreibungsdokument.pdf?__blob=publicationFile (accessed 30 November 2015).

76 Ulrich Grillo, "Wege zur digitalen Republik", *Handelsblatt*, 28 August 2015.

77 Annegret Bendiek, *Kritische Infrastrukturen, Cybersicherheit, Datenschutz. Die EU schlägt Pflöcke für digitale Standortpolitik ein*, SWP-Aktuell 35/2013 (Berlin: Stiftung Wissenschaft und Politik, June 2013).

78 Federal Office of Information Security and Federal Office of Civil Protection and Disaster Assistance, *Bund-Länder Kooperation*, http://www.kritis.bund.de/SubSites/Kritis/DE/Aktivitaeten/Nationales/BundLaender/bundlaender_node.html (accessed 5 February 2016); Bavarian State Parliament, *Schriftliche Anfrage des Abgeordneten Georg Rosenthal SPD vom 3. Dezember 2014.Zur Sicherheit kritischer Infrastruktur in Bayern*, Drucksache 17/5186 (Munich, 27 March 2015).

79 An offensive weapon may be defined as "[a]n act or action initiated in cyberspace to cause harm by compromising communication, information or other electronic systems, or the information that is stored, processed or transmitted in these systems." NATO, *Report on Cyber Defence Taxonomy and Definitions*, Enclosure 1 to 6200/TSC FCX 0010/TT-10589/Ser: NU 0289.

80 Federal Ministry of Defence, *Verteidigungspolitische Richtlinien. Nationale Interessen wahren – Internationale Verantwortung übernehmen – Sicherheit gemeinsam gestalten* (Berlin, 27 May 2011).

81 Quoted by Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF), "FIfF fordert einen öffentlichen Diskurs über die neue Cyber-Sicherheitsstratgie der Bundeswehr", Presseerklärung (Bremen, 15 July 2015).

82 James Andrew Lewis and Götz Neuneck, *The Cyber Index. International Security Trends and Realities* (New York and Geneva: United Nations Institute for Disarmament Research [UNIDIR], 2013, http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf (accessed 30 November 2015).

on international cyber and security policies: in between manufacturers of armoured vehicles, remote-controlled drones and two-way radios, participants meet IT companies such as McAfee, FireEye, Kaspersky, Symantec and Microsoft as well as relevant start-ups offering highly specialised services. It is hardly surprising, therefore, that the private IT security industry will have an annual turnover of around 155 million US dollars by 2020, according to estimates by the consulting firm Frost & Sullivan.[83] This market, which is developing fairly independently, offers "security as a service"[84]; its reverse side is "crime as a service".

83 Krzysztof Rutkowski, *Global Cybersecurity Market Assessment. National Strategies Drive the Adoption of Cyber Solutions* (17 February 2014), http://www.frost.com/sublib/display-report.do?id=M875-01-00-00-00 (accessed 30 November 2015).
84 "Security as a service" (SECaaS) as a special case of "software as a service" means making IT security provisions available over the Internet and is a form of security-critical IT outsourcing. Christian Senk, *Akzeptanz von Security-as-a-Service-Lösungen* (Berlin: Bitkom, 2011).

Cyber Policies Characterised by Due Diligence

The due diligence norm has direct relevance for strategic areas of Germany's international cyber policy and cybersecurity policy. Germany, the EU and NATO have so far been pursuing a defensive cyberstrategy in these areas. This differentiates Germany from individual EU and NATO partners such as France, Great Britain, the Netherlands and the US, which bank on deterrence through threats of retaliation and on surveillance and control technologies. Disastrous decisions on retaliation and escalation based on misinterpretations could potentially result from this, since technical, political and legal reasons make it almost impossible to identify attackers. For these reasons, cyberinsecurity is growing within the international community. States are users of ICTs; they have to protect their citizens and data; and at the same time they have to regulate the digital sector, which is largely dominated by private companies. Creating universally secure components is considered extremely difficult, but where software is used by the state, transparency, testing and analysis are indispensable. One can deduce from this state of affairs which are the most important areas of an international cybersecurity policy: human-rights and data protection policy; Internet Governance, fighting cybercrime; and developing international norms. These five areas overlap both conceptually and in terms of content. Unsurprisingly, problems arise from this, such as a conflictual coordination of responsibilities, or inconsistencies and a lack of coherence in the policies which are supposed to deal with challenges in cyberspace. In all of these areas, due diligence means taking to heart the three demands of European cooperation, inclusiveness and civilian response.[85]

Human Rights and Data Protection

Civil liberties on the Internet are constitutive of liberal democracies.[86] However, it is also clear – at the very latest since the revelations made by the former NSA employee Edward Snowden in 2013 – that even western secret services carry out passive surveillance on a massive scale and, moreover, that they knowingly infiltrate and compromise computer systems. Organisations such as Freedom House with its annual study Freedom on the Net, Reporters without Borders, or activists for free software remind us again and again that governments and globally active IT corporations do not provide continual barrier-free Internet access across the world. These organisations claim, for instance, that the Facebook project Internet.org only gives access to Facebook. Freedom activists demand that Internet access should be a basic human right; at the UN, however, discussions on this topic are far from reaching a conclusion.[87]

In a July 2012 resolution, the UN Human Rights Council emphasised that human rights are valid in the same way online as they are offline.[88] In November 2013, as part of a German-Brazilian initiative, the UN General Assembly adopted a resolution on privacy in the digital age, in which, among other things, it proscribes mass surveillance as illegal and undemocratic.[89] In May 2015, the UN's special rapporteur on freedom of expression, David Kaye, called for the encryption of private communications to be made a standard. In early July of the same year, the UN Human Rights Council created the post of UN special rapporteur on privacy and appointed Joseph Cannataci of Malta.[90]

85 In choosing the following topics for an international cyber and security policy, I make no claim to exhaustiveness. The examples listed only serve to illustrate the requirements named, which each policy would have to meet according to due diligence principles.

86 Ben Wagner, "Freedom of Expression on the Internet: Implications for Foreign Policy", *Global Information Society Watch* (2011): 20–22.

87 Ben Wagner, "Könnt ihr mich hören?", *Süddeutsche Zeitung*, 15 September 2015.

88 United Nations General Assembly, Human Rights Council, *The Promotion, Protection and Enjoyment of Human Rights on the Internet*, A/HRC/20/L.13 (New York, 29 June 2012), http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session20/A.HRC.20.L.13_en.doc (accessed 9 December 2015).

89 United Nations General Assembly, *Third Committee Approves Text Titled "Right to Privacy in the Digital Age", as It Takes Action on 18 Draft Resolutions*, GA/SHC/4094 (New York, 26 November 2013), http://www.un.org/press/en/2013/gashc4094.doc.htm (accessed 9 December 2015).

90 As early as 2014, the UN High Commissioner for Human Rights published a comprehensive report on privacy in the digital era. United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age. Report of the Office of the United Nations High Commissioner for Human Rights*, A/HRC/27/37 (New York, 30 June 2014).

However, democracies occasionally react to grave threats, such as Islamist terrorism, by declaring a state of emergency, as the US did after 9/11 or France after the Paris terror attacks of November 2015. One commentator remarked that "proof of the maturity of the law" lay in in maintaining the equilibrium between civil liberties and security measures during states of emergency.[91] The mission of the UN's new special rapporteur is to report on this equilibrium as it relates to privacy.

European Cooperation

The European experience has taught us that, in the long term, integrated economic areas also need integrated domestic and justice policies. The Lisbon Treaty gives great weight to the realisation of an "area of freedom, security and justice". Basic rights were strengthened by a Charter of Fundamental Rights, which was legally binding on the EU and came into force at the same time as the 2009 Lisbon Treaty, and by the obligation on the EU to ratify the European Convention for the Protection of Human Rights and Fundamental Freedoms. What holds true for the single market also holds true for the transatlantic economic area. Where the transfer of economic data is concerned, the EU and USA have agreed to finalise a so-called Privacy Shield. Current negotiations concern a transatlantic agreement on data protection in criminal prosecution, which might include steps towards harmonising criminal offences and a reciprocal hand-over of relevant data and information. Intensive cooperation among law-enforcement agencies is urgently needed to fight cybercrime. Online sources of funds for terrorism, such as digital financial services providers, can only be removed if the US and Europe cooperate closely on information sharing. A strengthened Terrorist Finance Tracking Program (TFTP), the umbrella agreement on data protection for law-enforcement purposes and modernised mutual legal assistance agreements (MLAs) are relevant steps forward for a constructive cooperation.[92] Fighting terrorism also requires comprehensive cooperation between the security services (as for instance between the "Five Eyes"[93]), which must, however, be subject to more stringent parliamentary controls. It is not in the interests of due diligence to have secret services exchange their insights informally and, in so doing, circumvent legal procedures, for instance those stipulated in agreements providing for mutual legal assistance.[94]

Inclusiveness

The more legally binding that regulations on human rights and data protection are, the more crucial it is to have laws implemented in an inclusive manner. That, at least, has been the experience in the EU. In Germany and Europe, data protection is directly linked to the right to informational self-determination whereby citizens have a say in how their personal data may be used. This right far exceeds the norm of due diligence, because the state has a duty of protection towards its citizens that it must fulfil. Technically speaking, data protection and the state's protective duties associated with it differ by area: international economic inter-

91 Andreas Zielcke, "Reifeprüfung des Rechts", *Süddeutsche Zeitung*, 3 December 2015.

92 European Union, *Agreement between the European Union and the United States of America on the Processing and Transfer of Financial Messaging Data from the European Union to the United States for the Purposes of the Terrorist Finance Tracking Program*, L 195/5 (Brussels, 27 July 2010); Council of the European Union, *Proposal for a Directive of the Council and the European Parliament on the Use of Passenger Name Record Data for the Prevention, Detection, Investigation and Prosecution of Terrorist Offences and Serious Crime*, 14670/15 (Brussels, 2 December 2015).

93 This is the most significant secret-services cooperation in the world, between the USA, Great Britain, Canada, Australia and New Zealand. On this subject, see e.g. European Parliament, *Report on the Existence of a Global System for the Interception of Private and Commercial Communications (ECHELON Interception System)* (2001/2098(INI), A5-0264/2001 (Brussels and Strasbourg, 11 July 2001). On the comprehensive cooperation between secret services in fighting transnational terrorism, see Katarina Zivanovic, "International Cooperation of Intelligence Agencies against Transnational Terrorist Targets", *PfP Consortium Quarterly Journal* 8, no. 1 (2008): 115–41; Richard J. Aldrich, "International Intelligence Cooperation in Practice", in *International Intelligence Cooperation and Accountability. Studies in Intelligence*, ed. Hans Born, Ian Leigh and Aidan Wills (New York: Routledge, 2010): 18–41.

94 Council of the European Union, Agreement with the United States on mutual legal assistance, 2009/820/GASP (Brussels, 23 October 2009); German Federal Parliament, *Gesetz zu dem Abkommen vom 25. Juni 2003 zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über Auslieferung, zu dem Abkommen vom 25. Juni 2003 zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über Rechtshilfe, zu dem Vertrag vom 14. Oktober 2003 zwischen der Bundesrepublik Deutschland und den Vereinigten Staaten von Amerika über die Rechtshilfe in Strafsachen, zu dem Zweiten Zusatzvertrag vom 18. April 2006 zum Auslieferungsvertrag zwischen der Bundesrepublik Deutschland und den Vereinigten Staaten von Amerika sowie zu dem Zusatzvertrag vom 18. April 2006 zum Vertrag zwischen der Bundesrepublik Deutschland und den Vereinigten Staaten von Amerika über die Rechtshilfe in Strafsachen (G-SIG: 16019368)* (Berlin, 26 October 2007).

dependence, the fight against crime and secret-service cooperation. Specific arrangements are made in each of these areas because of the threat each poses to individual freedoms and security; these arrangements in turn have an impact on how inclusive the regulations are.[95]

Data protection has become an area of law for which responsibility within the EU is divided. Legally binding data protection provisions between states have so far only been concluded at a regional level, namely in 1981 in the shape of the European Council's convention on data protection.

The trialogue between representatives of the Commission, the European Parliament and the Council of the European Union led to an agreement in December 2015 on a package of reforms for data protection in the shape of the General Data Protection Regulation (GDPR[96]), which replaced the EU's data protection directive of 1995. The new Regulation will have to be transposed directly into national law as of 2018. The GDPR reform package includes a directive that stipulates a harmonised legal framework for rules on data processing by the police and judicial authorities of the EU member states. The GDPR will outlaw the passing-on of data gathered in the EU for commercial or other uses to courts or authorities of third states. The best-known examples of this practice are the large digital-service providers such as Amazon, Google and Facebook, which store the data of European clients in the US using data protection provisions that violate European law. Where there are grave violations of the data protection law, data protection authorities will in future be able to impose drastic fines on companies. Such authorities are playing an ever more important role as instances for complaints and control because they verify how personal data are handled and can initiate sanctions.[97] Their independence therefore needs to be reinforced and the influence of private-sector companies on them needs to be restricted. The ECJ has clarified in two decisions (2010 and 2012) that data protection officials and their agencies must enjoy "complete independence".[98]

Civilian Response

The data required to launch a criminal prosecution are not only generated through IT methods in the respective country. Any EU member state launching a prosecution will also always access data sources that were generated in allied states under different legal circumstances and do not meet the strict German or European requirements for data protection. While increased retention of data is viewed as an important instrument in fighting cybercrime, it has been inadmissible to inform on or survey transmission data generated in the past since the German Federal Court's decision of 2 March 2010. On 8 April 2014, the ECJ also quashed the EU directive on data retention, arguing that it was incompatible with the EU Charter of Fundamental Rights. A draft law presented by Federal Justice Minister Heiko Maas in 2015 intends to store the telecommunications data of all German citizens for 10 weeks.[99] Technically, the instrument is already almost outdated.

95 Alongside the relevant paragraphs in Germany's Basic Law, the legal bases can be found in the primary legislation on the security services, police and other authorities: Bundesdatenschutzgesetz (BDSG), Telekommunikationsgesetz (TKG), Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz – G10), Gesetz über das Bundeskriminalamt (BKAG), Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSIG), Gesetz über das Zollkriminalamt und die Zollfahndungsämter (Zollfahndungsdienstgesetz – ZFdG), Gesetz über den Bundesnachrichtendienst (BND-Gesetz – BNDG), Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (Bundesverfassungsschutzgesetz – BVerfSchG), Gesetz über den Militärischen Abschirmdienst (MAD-Gesetz – MADG), Verordnung über die Übermittlung von Auskünften an die Nachrichtendienste des Bundes (Nachrichtendienste-Übermittlungsverordnung – NDÜV).

96 Council of the European Union, *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, document 5455/16 (Brussels, 28 January 2016).

97 The federal commissioner for data protection and freedom of information is expected to control the data protection efforts of telecommunications and postal services providers, federal agencies and other public federal offices. Unlike his or her colleagues at the state level, he or she will only be able to caution offenders, but not fine them.

98 European Court of Justice, Judgment of the Court (Grand Chamber). *Failure of a Member State to fulfil obligations – Directive 95/46/EC – Protection of individuals with regard to the processing of personal data and the free movement of such data – Article 28(1) – National supervisory authorities – Independence – Administrative scrutiny of those authorities.* Case C-518/07 (Luxembourg, 9 March 2010); European Court of Justice, Judgment of the Court (Grand Chamber). *Failure of a Member State to fulfil obligations – Directive 95/46/EC – Processing of personal data and free movement of such data – Protection of natural persons – Article 28(1) – National supervisory authority – Independence – Supervisory authority and the Federal Chancellery – Personal and organisational links.* Case C-614/10 (Luxembourg, 16 October 2012).

99 This does not apply to phone bugging undertaken by the

In any case, big data[100] is becoming increasingly interesting for criminal prosecutions as well.[101] Existing data sources, algorithms and predictive analytics are used for this.[102] A further method is source telecommunication surveillance, which is the authorities' response to increasing communications encryption[103] at the federal level.[104]

For this, investigating authorities install a programme nicknamed 'the Federal Trojan" on suspects' computers.[105] Emails, Internet telephony or chats can then be recorded directly within the system and transferred before the programme encrypts the communication. The Federal Trojan is controversial because it could be considered a cyberweapon, whose use would in that case have to be authorised by Parliament. It is possible that more cooperation between authorities and academia would be helpful in better judging and categorising the facts. In the field of prevention, the Federal Government started an interdepartmental research programme on improving security in cyberspace in March 2015. Its focal points are (1) new technologies, (2) security and trustworthy information and communications systems, (3) areas of application for security and (4) privacy and data protection. The German Federal Ministry of Education will fund the programme, entitled "Secure and self-confident in the digital world", with about 180 million euros until 2020.[106]

police for preventative purposes or to breaches by the intelligence services of telecommunications confidentiality where these are not under judicial oversight. Preventative police work is covered by the BKA Law of 25 December 2008. Gerd Lehmann, "Wie geht es jetzt – wie in Zukunft?", *Behörden Spiegel* (July 2015).

100 The expression "big data" describes the automated, computer-supported processing of large and heterogenous volumes of data. It has great potential, in particular for industry and the empirical sciences. Federal Ministry of Education and Research, *Big Data – Management und Analyse großer Datenmengen*, http://www.bmbf.de/de/big-data-management-und-analyse-grosser-datenmengen-851.html (accessed 5 February 2016).

101 An example is the Child Abuse Prevention System (CAPS) software, operated by the Diplomatic Council, a global think tank with special-advisor status at the UN. CAPS complements existing infrastructure, processes and solutions of prosecuting authorities across the world and supports the White IT alliance, which fights child pornography. Mass surveillance, unjustified general suspicion and the displacement of resources from personnel to technical solutions are considered to be the problematic side effects of the new prosecution techniques. James Byrne and Gary Marx, "Technological Innovations in Crime Prevention and Policing. A Review of the Research on Implementation and Impact", *Cahiers Politiestudies* 3, no. 20 (2011): 17–40 (32).

102 Walter L. Perry, Brian McInnis, Carter C. Price, Susan C. Smith and John S. Hollywood, *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations* (Santa Monica: RAND Corporation, 2013).

103 On this point, see Sandvine, ed., *Global Internet Phenomena Spotlight: Encrypted Internet Traffic* (Waterloo, Ontario, 2015), http://www.sandvine.com/downloads/general/global-internet-phenomena/2015/encrypted-internet-traffic.pdf (accessed 5 February 2016).

104 In its Digital Agenda 2014–2017, the German Federal Government set itself the target of creating "security and protection on the Web". It even announced its intention of becoming the "world's no. 1 location for encryption".

105 German Federal Parliament, *Kleine Anfrage der Abgeordneten Jan Korte, Andrej Hunko, Ulla Jelpke, Petra Pau, Jens Petermann, Frank Tempel, Halina Wawzyniak und der Fraktion Die Linke. Auskunft über Einsatz staatlicher Schadprogramme zur Computerspionage ("Staatstrojaner")*, Drucksache 17/7104 (Berlin, 25 October 2011).

Internet Governance

The mission of Internet Governance is to agree technical standards and rules for the cross-border connectivity of national networks.[107] The substantial challenges here consist of guaranteeing the availability, confidentiality, authenticity and integrity of data. In its Digital Agenda 2014–2017,[108] the German Federal Government supports the continuation of the multi-stakeholder approach in Internet Governance. The way Germany proceeds in Internet Governance[109] must be coordinated with other European states. Weak points in hardware and software products as well as issues of cryptology must also be discussed. In Internet Governance, the stakeholders – private users, the civil society, academia, companies and governments – are expected to act responsibly in their respective roles and participate in developing the Internet. This is intended to ensure that the decisions taken have a broad base of legitimacy.

Important components of a functioning and reliable Internet-governance system are international organisations and fora such as the Internet Corporation for Assigned Names and Numbers (ICANN), which

106 Federal Ministry for Education and Research, ed., *Selbstbestimmt und sicher in der digitalen Welt 2015–2020. Forschungsrahmenprogramm der Bundesregierung zur IT-Sicherheit* (Bonn and Berlin, 2015).

107 Federal Parliament, *Aktueller Begriff. Internet Governance*, Drucksache 11/14 (Berlin, 27 March 2014). Debates about the use and further development of the Internet use as their basis the Internet model that combines network zones of the Internet and technical levels of communication.

108 BMWi/BMI/BMVI, *Digitale Agenda 2014–2017* (see note 65).

109 Internet Society, *IANA Transition*, http://www.internetsociety.org/ianaxfer (accessed 5 February 2016).

is responsible for the stable functioning of the Internet; the Information Society (ISOC); the Organisation for Economic Cooperation and Development (OECD); and the Internet Governance Forum (IGF), a multi-stakeholder forum with 3,700 members from 144 countries, which was established following the UN World Summit on the Information Society.[110] States should only intervene in a regulatory capacity when self-regulation can no longer guarantee democratic legitimacy, effectiveness, rule of law and transparency. Multilateral cooperation comes into play whenever concerns of states with less developed Internet capacities are to be integrated into Internet Governance. In Germany, the Federal Ministry for Economic Affairs and Energy will be in overall control of the future of Internet Governance and Industrie 4.0. A series of reforms of Internet Governance can be inferred from the due diligence standard:

European Coordination

The German Federal Government should coordinate its national position with its EU partners and other states, especially the OECD, to create the preconditions for asserting its views internationally at the UN (as it did, most recently, at the WSIS follow-up conference in December 2015). It is pointless to stand alone, for the simple reason that Germany does not have sufficient negotiating power in the multilateral or Internet Governance fora. The EU position was set in June 2011 when the European Commisssion declared that the EU's aim was to create "a single, un-fragmented network, subject to the same laws and norms that apply in other areas of our day-to-day lives".[111] The EU and Germany are in favour of a leading role for the Internet Governance Forum, whose term was extended by another five years at the UN summit in December 2015. This is intended to prevent intergovernmental influence from being exerted to the disadvantage of the multi-stakeholder approach, and to "internationalise" bodies and functions such as ICANN and IANA (Internet Assigned Numbers Authority). By this, the EU means engaging in an inclusive dialogue with developing, emerging and industrialised countries in terms of innovative best practices, with the goal of ensuring Internet access even in rural areas (capacity-building). With the help of Internet Governance, it wants to continually improve ICT even in less developed regions and parts of the world.

Inclusiveness

Inclusiveness and legitimacy are highly controversial in global Internet Governance.[112] However, civil-society interest groups and members of parliament ought to be involved in the setting of global Internet norms, so that decisions are not only taken by technical bodies such as the Internet Architecture Board. Inclusiveness is the only guarantee that the necessary professional competence will be made available and that social acceptance for the norm-setting processes will be generated. Beyond this, IANA's function of assigning top-level domains – meaning the highest level of name resolution, such as *.com or *.de – should be put on a footing acceptable to all. The multi-stakeholder process in Internet Governance has been extended for five years because the UN General Assembly decided in late 2015 that the IGF should continue its activities.[113] The security issues of individual governments, such as Russia or Saudi-Arabia, are inevitably playing an ever greater role in questions of Internet administration.[114]

Civilian Response

The preconditions for civilising digital communications are confidentiality, integrity and reliability.

110 Correct as of 2014. See IGF website, http://www.intgovforum.org/cms/ (accessed 5 February 2016).

111 The relevant acronym is COMPACT (*C*ivic Responsibilities, *O*ne Unfragmented Resource, *M*ultistakeholder Approach to *P*romote Democracy and Human Rights, Sound Technological *A*rchitecture, *C*onfidence and *T*ransparent Governance). European Commission, *Internet Policy and Governance Europe's Role in Shaping the Future of Internet Governance*, COM(2014) 72 final (Brussels, 12 February 2014), http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52014DC0072&from=EN (accessed 30 November 2015).

112 Annegret Bendiek, Christoph Berlich and Tobias Metzger, *Die digitale Selbstbehauptung der EU*, SWP-Aktuell 71/2015 (Berlin: Stiftung Wissenschaft und Politik, August 2015), 6f.

113 United Nations General Assembly, *Outcome Document of the High-level Meeting of the General Assembly on the Overall Review of the Implementation of the Outcomes of the World Summit on the Information Society*, A/70/L.33 (New York, 13 December 2015).

114 Monika Ermert, "WSIS+10: Zehn Jahre nach dem großen Gipfel", *heise online*, 14 December 2015, http://www.heise.de/newsticker/meldung/WSIS-10-Zehn-Jahre-nach-dem-grossen-Gipfel-3043 792.html (accessed 5 February 2016).

Communication occurs in a global network of networks, whose servers are distributed all over the world. The location of each server therefore has little impact on the security or privacy of communications. Established certification standards are much more important. Users can encrypt emails, establish single-use email adresses[115] or rely on De-mail.[116] Nevertheless, states are claiming the right to access encrypted communications in criminal prosecutions and therefore to build "backdoors"[117] into the systems of suspects. Even well-encrypted emails generate metadata, which yield a lot of information about their sender, receiver, subjects and time. Security services such as the NSA collect such data on a grand scale. Much work is being carried out on encryption technologies to make this task more difficult.[118] Users themselves play a decisive role in civilising communications. They can exert pressure to help enforce a user-friendly, sophisticated and fully differentiated encryption. It therefore makes sense for the Internet Governance committees to discuss cybersecurity more and more often as well. It would be inadvisable, however, to securitise Internet Governance or to allow states to exert increasing influence over it, with the exception of state bodies wanting to comply with due diligence. Fundamentally, however, Internet Governance remains in the hands of private actors for the time being.

Fighting Cybercrime

The fight against cybercrime encompasses all non-military measures that protect civilian targets from digital attackers. First and foremost, this concerns critical infrastructure and personal civil rights (and liberties). Since the 9/11 attacks, the UN has passed a great number of resolutions in the fight against terrorism that could serve as points of departure for cybersecurity as well.

Germany has ratified the Council of Europe's Budapest Convention on Cybercrime[119] and backs the EU's cybersecurity strategy of February 2013.[120] which uses the same approach as Germany, namely a cybersecurity policy that is defensive and police-based in orientation. So far, the EU has limited itself to coordinating the effort to create "an open, secure and protected cyberspace" by focusing on a) creating resilient IT structures, b) fighting cybercrime, c) developing defensive cybercapacities, d) promoting industrial and technological developments in cybersecurity, and e) developing international cyberdiplomacy.[121] The success and prospects of Europe's internal security depend on it acting at the national, European and international levels whilst making use of the technological possibilities of information exchange between these levels and giving that exchange legal protection. The globalisation, automation and industrialisation of crime require international and European coordination, especially structural information exchanges between the prosecuting authorities.[122]

European Coordination

To enforce due diligence in the fight against cybercrime, substantive criminal law must urgently be harmonised, above all the definition of a criminal offence. Most EU member states have signed the Budapest Convention and thus committed themselves to prosecuting offences occurring in cyberspace. However, the legal conceptions of EU countries vary wildly when it comes to deciding which actions in cyberspace

115 Provisional email addresses are also offered under the names of disposable email or instant email. They are intended as much as possible to limit the loss of personal data when a loss of integrity, meaning a falsification of information, occurs with website operators.

116 The Federal Government implemented the European directive 2006/123/EC on service provisions in the internal market via the De-Mail (De-Mail-G, 28 April 2011). Using De-mail, messages and documents can be sent and received confidentially, securely and verifiably. De-mail is offered by various e-mail providers in Germany and can be used, among other things, for digital correspondence with many ministries. *E-Mail made in Germany. Eine Initiative von GMX, Telekom und WEB.DE*, http://www.e-mail-made-in-germany.de/index.html (accessed 5 February 2015).

117 "Backdoor" is the name given to weak points deliberately inserted into hardware and software, which make it possible to access certain functions of the computer or software in question at a later date.

118 See for instance Johannes Wendt, "Wie Dark Mail die Metadaten abschaffen will", *Zeit Online*, 7 January 2015, http://www.zeit.de/digital/datenschutz/2015-01/darkmail-verschluesselung-meta daten-email-lavabit (accessed 30 November 2015).

119 Council of Europe, *Convention on Cybercrime*, CETS No. 185 (Budapest, 23 November 2001).

120 European Commission, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, JOIN (2013) 1 final (Brussels, 7 February 2013).

121 Ibid., 4f.

122 "Digitale Agenda", interview with Boris Pistorius, Minister of the Interior of Lower Saxony, *Behörden Spiegel* (February 2014).

should be rated crimes and how they should be punished. It would not be appropriate to harmonise criminal offences using intergovernmental agreements of individual state's regulations. Rather, what is needed is a process that involves all EU states and orientates itself on the due legislative processes of the EU.

As of yet, however, the EU does not have the authority to harmonise criminal law. Its current legal and political system still rests on criminal law applying and operating within national borders. At the same time, it is becoming more difficult to categorise access rights because cloud services, for example, operate beyond continent. The EU should nevertheless concentrate on the issue of criminal prosecution while applying the "European agenda on security". There are a number of further meaningful initiatives, such as the European arrest warrant, the creation of a European prosecution service or the adoption of mutual legal assistance agreements, including all relevant transatlantic agreements. To disincentivise companies from relocating their business abroad and thus circumventing due diligence obligations, the EU's data-security standards (the NIS directive) should be brought into line with those set in the US by the National Institute of Standards. Transatlantic cooperation has an important role to play not only in public-private partnerships, but also at the official level, for instance in the EU-US working group on fighting cybercrime.[123]

Inclusiveness

Security agencies on the EU and national levels will have to get used to the fact that the fight against cybercrime can no longer dispense with the cooperation of private actors. A clear separation between private and public sector can hardly be upheld in this area, because the companies that have been attacked are frequently the only bodies that have the means of resolving cyber attacks. Corporations like Microsoft even obtain court orders authorising so-called hackbacks: authorising them, in other words, to penetrate the attackers' IT systems in turn, for instance to destroy groups of automated malware, so-called botnets.[124] While it remains difficult to attribute cyber attacks unequivocally – for instance, because of falsified invoices, sabotaged computer systems and password theft – perpetrators nonetheless leave digital traces. Reconstruction and analysis – IT forensics – are thus the pivot of criminal prosecution.[125] The German authorities, including the BKA and the state bureaux of investigation, therefore back the action plan of the European Police Office (Europol).[126] Today, prosecuting authorities also systematically look for dangers in the IT system (threat hunting), instead of merely reacting to attacks. Where such a hunt is successful, attackers may be prevented from accessing the most sensitive areas. However, this presupposes that data is stored in such a way that it can be used in court. Gathering evidence from large and complex data banks takes time and requires extremely powerful computers. Digital forensics face enormous challenges. That is why authorities bank on support from private IT forensic scientists to solve crimes. But public-private cooperation on cybersecurity has its weak points, among other reasons because industry has so far not markedly got involved in fighting crime, except for the BSI initiative Allianz für Cyber-Sicherheit and for CERT exchanges. The Global Player Initiative is a network founded back in 2006, in which the BKA and (currently) 62 large enterprises participate. Overall, the BKA cooperates with about 630 companies. Frequently, this exchange of information is still more of a one-way street, because small and medium enterprises in particular do not have the capacities for taking far-reaching IT-security measures. In Germany, operators of critical infrastructure are obliged to report cyber attacks and introduce minimum security standards for their IT. However, security issues concerning software products and external cloud services have not yet been sufficiently resolved. Binding security tests and an extension of the manufacturer's liability are currently under intensive discussion.[127]

123 Annegret Bendiek, *Umstrittene Partnerschaft. Cybersicherheit, Internet Governance und Datenschutz in der transatlantischen Zusammenarbeit*, SWP-Studie 26/2013 (Berlin: Stiftung Wissenschaft und Politik, December 2013); European Parliament, Directorate-General for Internal Policies, *Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses, Study for the LIBE Committee* (Brussels, 2015).

124 Janine S. Hiller, "Civil Cyberconflict: Microsoft, Cybercrime, and Botnets", *Santa Clara High Technology Law Journal* 31, no. 2 (2015): 163–214.

125 German Federal Office of Information Security, *Leitfaden "IT-Forensik"*, version 1.0.1 (Bonn, March 2011).

126 Federal Parliament, *Antwort auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Jan van Aken, Wolfgang Gehrcke, weiterer Abgeordneter und der Fraktion Die Linke, Maßnahmen im operativen Europol-Aktionsplan für das Jahr 2015 zu Cyberangriffen mit deutscher Beteiligung*, Drucksache 18/4585 (Berlin, 10 April 2015).

127 German Federal Office of Information Security, ed., *Die Lage der IT-Sicherheit in Deutschland 2015* (see note 27).

Civilian Response

In accordance with the EU's cybersecurity strategy, cybercrime shall be fought using exclusively non-military means. According to the strategy the relevant agencies need to be given more supranational competences and more funds. These include Europol's European Cybercrime Centre (EC3)[128]; the European Network and Information Security Agency (ENISA); and the European Union's Judicial Cooperation Unit (Eurojust). The cyberexercises that are regularly coordinated by ENISA may not be spectacular, but they are important for building resilient IT structures in accordance with due diligence. 29 EU-EFTA member states and 200 governmental organisations participated in the Cyber Europe 2014 exercise.[129] The exercise was designed to test how to improve cooperation between states in coping with cybersecurity incidents in the whole of Europe; how the many parallel communications relations impact on generating an overview of the national and European situation; and what consequences a comprehensive European cybercrisis might have for the member states' press and PR activities. At the operative level, the continuous cooperation of the IT emergency teams with other CERTs is indispensable. The BSI, for instance, is a member of the European Government CERTs Group (EGC), an informal group at the European level, and of the Forum for Incident Response and Security Teams (FIRST), an international coalition of about 200 state and private CERTS.[130]

Cyberdefence

The NATO centre for repelling cyber attacks, the Cooperative Cyber Defence Centre of Excellence (CCDCOE), is financed by 11 member states of the Alliance, but is not part of its command structure. In the Tallin Manual, which includes the work of German academics, the Centre presented proposals for codifying the right to war *(ius ad bellum)* and the law of war *(ius in bello)* for cyberspace.[131] Its authors also attempted to elaborate how due diligence might be best served in cyberspace. For example, the Tallinn Manual states that "[a] State shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States."

In line with its constitutional obligation to defend the Alliance, the German military also primarily has defensive cybercapabilities, meaning that it is geared for cyberdefence.[132] Cyberdefence includes measures for repelling threats not just against individual persons or enterprises but also against the state and its social foundations. The German armed forces view themselves as the central instance for repelling external dangers in cyberspace as well. According to Germany's security strategy, IT systems in military use and the German share of cyberspace are also part of cyberdefence. For some time now, it has been clear not only that digital conflicts are increasingly carried out in cyberspace, but also that military deployments are occurring below the threshold of armed conflict and that non-state actors are involved. The German Federal Government therefore explicitly points out that military actors may also be responsible for cyber attacks.

European Cooperation

Germany's cyberdefence policy should push for European and Atlantic cooperation early on, always with the aim of enforcing the guiding principle of due diligence. National measures intended to check and increase the quality of the components and key technologies in use should be based on the clarification and exchange of information within the EU, and between the EU and NATO. In December 2013, the European Council announced that it would intensify EU-NATO cooperation. In November 2014, it adopted the Cyber Defence Policy Framework.[133] This is intend-

128 Europol, *European Cybercrime Center (EC3)*, http://www.europol.europa.eu/content/megamenu/european-cybercrime-centre-ec3-1837 (accessed 5 February 2016).
129 European Network and Information Security Agency, *ENISA CE2014. After Action Report* (Heraklion, 2014).
130 European Government CERTs Group, *Members of the European Government CERTs Group*, http://www.egc-group.org/contact.html (accessed 30 November 2015); Forum for Incident Response and Security Teams, *FIRST Members*, http://www.first.org/members (accessed 30 November 2015).
131 Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (see note 9).
132 Federal Ministry of Defence, "Von der Leyen reformiert Cyber-Strukturen" (Berlin, 17 September 2015).
133 Council of the European Union, *EU Cyber Defence Policy Framework*, 15585/14 (Brussels, 18 November 2014), http://www.europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede160315eucyberdefencepolicyframework_/sede160315eucyberdefencepolicyframework_en.pdf (accessed 3 December 2015).

ed to increase the protection for missions of the Common Security and Defence Policy (CSDP) and the security of communications in the European External Action Service (EEAS).[134]

In its strategic concept of 2010, NATO declared that cyber attacks can "reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability".[135] As a result, at its summit in Wales in June 2014, the Alliance adopted its Enhanced Cyber Defence Strategy, with the aim of building resilient ICT-structures in the military field.[136] Alongside consultation and support processes, there will also be joint exercises, for instance on handling cyber attacks. Every year, NATO Computer Incident Response Capability (NCIRC), which has also been entrusted with operative IT security and network surveillance, organises its three-day Cyber Coalition.[137] The NCIRC Coordination Centre is responsible for coordinating with member states and partner organisations for this event, such as the EU, OSCE or International Telecommunication Union (ITU). Cooperation between NATO and the EU-CERT has also been decided.[138] European cooperation in cyberdefence comprises research as well as industry as a "first line of defence".[139]

134 European External Action Service, *EU International Cyberspace Policy*, http://eeas.europa.eu/policies/eu-cybersecurity/ (accessed 5 February 2016).

135 NATO, *Active Engagement, Modern Defence. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization* (Brussels, 2010), http://www.nato.int/strategic-concept/pdf/Strat_Concept_web_en.pdf (accessed 2 December 2015).

136 "The policy reaffirms the principles of the indivisibility of Allied security and of prevention, detection, resilience, recovery, and defence." NATO, "Wales Summit Declaration", Pressemitteilung 120/2014 (5 September 2014), http://www.nato.int/cps/en/natohq/official_texts_112964.htm (accessed 3 December 2015).)

137 The CCDCOE exercise "Locked Shields" should also be mentioned here.

138 Andreas Wilkens, "EU und NATO kooperieren enger im Kampf gegen Cyber-Terrorismus", *heise online*, 10 February 2016, http://www.heise.de/newsticker/meldung/EU-und-Nato-kooperieren-enger-im-Kampf-gegen-Cyber-Terrorismus-3098911.html?wt_mc=rss.ho.beitrag.atom (accessed 15 March 2016).

139 According to Alexander Vershbow, NATO Deputy Secretary-General, quoted on the website of the NATO Industry Cyber Partnership Forum, http://www.nicp.nato.int/ (accessed 3 December 2015).

Inclusiveness

Armed forces may only be deployed in cyberspace under the same conditions of constitutional law that apply to conventional military capabilities. In Germany, this concerns primarily Art 87a GG and Art 24 para 2 GG. If these preconditions are met, it is legally possible to take damaging (counter-)measures against an attacker's IT systems, including information-gathering and reconnaissance. Furthermore, the German armed forces can use their own capacities to protect the whole state from IT attacks. The legal basis for this is Art 35 para 1 GG and regulations on the use of the armed forces to repel and cope with a particularly grave incident. However, each armed deployment of German military forces requires the assent of the German Parliament under a law known as the Parlamentsbeteiligungsgesetz.[140] In developing a German cyberdefence policy, it is therefore advisable to reflect early on about involving the Federal Parliament. The legal precondition of parliamentary approval that exists in Germany is a major asset that must not carelessly be sacrificed to technological progress. In this context, there needs to be a debate on parliamentary approval after the fact, which was legitimised by the Federal Constitutional Court in its so-called Nafurah decision[141] in the summer of 2015. This dealt with the possibility of informing the German Parliament only in retrospect in cases where there is "Gefahrenverzug", meaning looming danger.

Civilian Response

In times of peace, due diligence in cyberdefence means pursuing primarily civilian approaches to the preventative and reactive protection of one's IT systems and infrastructure. However, Germany is also arming itself militarily for cyberspace. Since December 2011, the German military's unit for computer network operations[142] has had an initial capability,

140 German Federal Parliament, *Gesetz über die parlamentarische Beteiligung bei der Entscheidung über den Einsatz bewaffneter Streitkräfte im Ausland (Parlamentsbeteiligungsgesetz, ParlBG)* (Berlin, 18 March 2005).

141 This was triggered by the participation of the German armed forces in an evacuation operation in Libya in 2011. Constitutional Court, *Urteil des Zweiten Senats vom 23. September 2015 – 2 BvE 6/11 – Rn. (1–125)*.

142 Kommando Strategische Aufklärung, *Über uns*, 25 November 2013.

meaning "a degree of personnel and material readiness for duty [...], which makes it possible, within limits, to have an impact through cyberspace".[143] Thus, several battalions with different tasks in electronic warfare report to the strategic reconnaissance commando (KSA).[144] During the elaboration of the 2016 White Paper, defence minister von der Leyen announced that the German armed forces were establishing a cyberspace and information-space division (CIR).[145] It is certain that cyberspace, as the fifth operational domain alongside land, air, sea and space, will have an impact on the German military's deployability. To avoid a digital arms race,[146] cyberdefence needs to focus above all on building resilient structures.[147] However, improved defensive capacities are not enough. It is also essential to develop high-security IT in close collaboration with other EU states and allies, and to curb the worldwide "black market" for vulnerabilities in IT systems, and especially zero-day markets.[148]

However, even within the German armed forces there are concerns that the new division (CIR) could develop in ways that are similar to the United States Cyber Command (USCYBERCOM), which is not subject to any parliamentary oversight and works closely with the NSA. There are concerns that the activities of the CIR cannot be reconciled with the traditional understanding of the "citizen in uniform". The manner in which the capabilities to be created are strategically and operationally integrated into the German armed forces will therefore be decisive.

Developing International Norms

Developing international norms is a central part of Germany's international cyber policy. Germany exports technological products worldwide and receives primary products from almost all of the world's countries. However, since adjusting to standards always has its costs, it is very much in Germany's interests wherever possible to turn its own standards into the international norm. For this, its international cyber policy acts in three areas. Its first goal is to reach agreements with third parties on confidence and security-building measures. Its second aims is to conclude agreements that set international standards for the approval of hardware and software and define norms for responsible conduct by states. Its third target is applying international law in cyberspace.

European Cooperation

For the cyberdefence policy to enforce due diligence in cyberspace, the EU needs to be placed in a position where it can engage more closely in developing international norms. In April 2015, the EU's High Representative for Foreign Affairs and Security Policy, Federica Mogherini, and the Dutch Foreign Minister Bert Koenders emphatically pointed out the necessity of taking states up on their promise for their behaviour in cyberspace. Mogherini and Koenders believe that insufficiently secured central infrastructure is a threat to national and international security.[149] In this, they represent all 28 member states, which have agreed on this line in cyberdiplomacy.[150]

However, constructive criticism on the global level is extremely difficult because there are such divergent views throughout the world on various aspects of information security. Contentious areas include the range

143 Thomas Wiegold, "Cyber-Attacke auch für Deutschland ein möglicher Angriff nach dem Völkerrecht", *Augen geradeaus!* (Blog), 12 October 2012, http://augengeradeaus.net/2012/10/cyber-attacke-auch-fur-deutschland-ein-moglicher-angriff-nach-dem-volkerrecht/ (accessed 15 March 2016).
144 Federal Ministry of Defence, *Dienststellen der Streitkräftebasis, Kommando Strategische Aufklärung*, http://www.kommando.streitkraeftebasis.de/portal/a/kdoskb/!ut/p/c4/04_SB8K8xLLM9MSSzPy8xBz9CP3I5EyrpHK94uyk-OyUfL3s4kT9gmxHRQCRV4XQ/ (accessed 30 November 2015).
145 Federal Ministry of Defence, "Tagesbefehl der Ministerin: Bundeswehr wird im Cyber-Raum zukunftsfähig" (see note 45); Bundesministerium der Verteidigung, "Von der Leyen reformiert Cyber-Strukturen" (see note 132).
146 Ronald Deibert, "Tracking the Emerging Arms Race in Cyberspace", *Bulletin of the Atomic Scientists* 67, no. 1 (2011): 1–8.
147 Federal Parliament, first committee of inquiry, *Stenografisches Protokoll der 9. Sitzung*, 18. Wahlperiode (Berlin, 26 June 2014), http://www.bundestag.de/blob/372418/97c666605f875474927dfcf5b42c4fcb/09-waidner_gaycken_rieger_endgueltig-data.pdf (accessed 30 November 2015).
148 "A Zero Day Exploit Attack (ZETA) is an attack carried out on the same day as the software weak point is discovered. In this case, the weak point is exploited before the software manufacturer can close it with a fix." Kaspersky Lab, *Was ist ein Zero-Day-Exploit?*, http://www.kaspersky.com/de/internet-security-center/definitions/zero-day-exploit. See also Federal Office of Information Security, ed., *Die Lage der IT-Sicherheit in Deutschland 2015* (see note 27).

149 Bert Koenders and Federica Mogherini, "Cyber Space Needs Stronger Rule of Law", *EU Observer*, 16 April 2015, https://euobserver.com/opinion/128342 (accessed 16 March 2016).
150 Council of the European Union, *Council Conclusions on Cyber Diplomacy*, 6122/15 (Brussels, 11 February 2015).

of topics, threat perception and the role of the UN and governments, including vis-a-vis actors from the private sector and civil society. Germany is a prominent representative at all of these international debates. 20 states, including five EU member states, took part in the fourth round of the negotiations of governmental experts on information security (UN GGE).[151] The final reports of the expert rounds were adopted by the UN General Assembly. However, the concrete application of international law to cyberspace remains a point of contention. Selected EU states are engaging on the UN level and represent the EU. There is closer agreement between Europe's "Big Three" as well as bilaterally with the US and Israel in the group of likeminded western states (which alongside Germany, Spain, France and Great Britain also comprises Colombia, Israel, Japan, South Korea and the US). A fifth round of GGE negotiations is scheduled to start in 2016. The EU states involved should focus their energies on giving EU concerns more emphasis in the GGE in future, as stipulated in the Council's conclusions on cyberdiplomacy.[152] In this, the EU needs to speak "with one voice", because a divided EU would find it very difficult to assert its interests over those of the US, Russia or China.

Inclusiveness

It is part of the tasks of the German and EU international cyber policy and cyberdefence policy to prevent a digital arms race by prioritising civilian approaches and confidence-building measures. On the occasion of its OSCE presidency in 2016, Germany intends to adopt a new package of confidence- and security-building measures that particularly integrates science and the civil society.[153] Because of its experience in arms control and confidence-building that span opposing blocs, the German OSCE chairmanship is developing CSBMs in all three areas for cyberspace. The OSCE is a regional approach that complements and supplements the work of the GGE. It is expected to safeguard the mutual commitment that no computer systems or cyberinfrastructure on the territories of its member states will be used for attacks on other states. But provisions must also not be misused for restricting the freedom of the Internet. In partnership with science and companies, the OSCE intends to promote the development of protective measures that are both technical and regulatory to make critical infrastructure in OSCE states more resilient. Cybersecurity can only be guaranteed if stakeholders do so in coordination with national governments and the EU, and involve as many concerned parties as possible.[154] The EU approach of "inclusive multi-stakeholderism" is increasingly becoming the trademark of international cyber policy and digital diplomacy.

Civilian Response

The development of international norms raises political questions with direct relevance for the global assertion of human rights and for national security. Since June 2013, Germany has been a member of the Freedom Online Coalition, a multi-stakeholder platform that now comprises 28 countries and campaigns for liberties in cyberspace.[155] Due diligence also applies to German companies in the information, communications and Internet economy. They must therefore ensure that their exports are not used by authoritarian regimes to abuse civil liberties on the Internet. The German Federal Government should continue to work towards worldwide controls on the trade in digital

151 Antigua and Barbuda, Belarus, Brazil (Presidency), China, Colombia, Egypt, Estonia, France, Germany, Ghana, Israel, Japan, Kenya, Malaysia, Mexico, Pakistan, Russia, Spain, United Kingdom, USA.

152 Council of the European Union, *Council Conclusions on Cyber Diplomacy* (see note 150); Eneken Tikk-Ringas, *Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee 1998–2012* (Geneva: ICT for Peace, 2012).

153 Annegret Bendiek, Christoph Berlich and Tobias Metzger, *Drei Prioritäten für die Cyberdiplomatie unter dem deutschen OSZE-Vorsitz 2016*, SWP-"Kurz gesagt" (Berlin: Stiftung Wissenschaft und Politik, 5 November 2015), http://www.swp-berlin.org/publikationen/kurz-gesagt/drei-prioritaeten-fuer-die-cyberdiplomatie-unter-dem-deutschen-osze-vorsitz-2016.html (accessed 5 February 2016); Representation of the Federal Republic of Germany in the Russian Federation, *OSZE-Konferenz zur Cybersicherheit im Auswärtigen Amt*, 18 January 2016, http://www.germania.diplo.de/Vertretung/russland/de/__pr/mosk/osze-cyber-konferenz-aa-18012016.html (accessed 5 February 2016).

154 See Microsoft, *International Cybersecurity Norms* (2015), http://download.microsoft.com/download/7/6/0/7605D861-C57A-4E23-B823-568CFC36FD44/International_Cybersecurity_%20Norms.pdf (accessed 9 December 2015).

155 Freedom Online Coalition, *Freedom Online Coalition Chair's Summary*, Third Freedom Online Conference, Tunis, 16–18 June 2013, http://www.freedomonlinecoalition.com/wp-content/uploads/2014/04/3-Tunis-Chair-report-from-website.pdf (accessed 9 December 2015).

arms.[156] For this, highly-developed countries should extend the Wassenaar Agreement[157] on arms export controls as quickly as possible, so that the trade in digital arms will in future be subject to the same requirements as the trade in conventional war equipment. The first steps have been taken towards introducing international export-control mechanisms and incorporate surveillance technologies in sanctions packages. These approaches could be continued, at least on the regional level, using the EU's dual-use regulation.[158] In particular, the export of such products to countries with authoritarian regimes needs to be more strictly prohibited than before. To this end, a standardised definition of cyberweapons must be elaborated and monitoring regimes be conceived at the EU and UN levels.[159] For the time being, it is unlikely that governments will conclude multilateral international-law treaties, which provide a binding settlement on the use of cyberspace for military operations, based on the disarmament and arms control model. The reasons for this area lacking definition of the term "cyberweapons"; problems with implementation and verification; and the difficulty of attributing cyber attacks unequivocally under international law. Bilateral agreements, such as the one on fighting cybercrime concluded between the US and China, are evidently easier to push through.[160] Fundamentally, due diligence should be interpreted as being reciprocal, meaning that norms and rules should apply between individual states as well as between states and private companies, in particular with a view to espionage and other military purposes, such as hybrid warfare. Dual-use technology is an awkward subject in the cooperation between civilian and military actors as well as between public and private actors, especially in the transatlantic alliance. Euro-Atlantic cooperation would be a good prelude to committing states within the EU and NATO to reporting weak points in IT products to the manufacturers, rather than deliberately building in backdoors. It is undeniably common practice to use cyberweapons, such as zero-day exploits. At least, their use should be more strictly limited, by having to fulfil clear criteria. The proliferation of cyberweapons, however, must definitely be stopped.

156 Germany has ratified the arms trade treaty adopted by the UN General Assembly on 2 April 2013. German Federal Parliament, *Gesetz zu dem Vertrag vom 2. April 2013 über den Waffenhandel* (Berlin, 19 October 2013).

157 See *The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies* (The Hague, 19 December 1995), http://www.wassenaar.org/december-1995-declaration-at-the-peace-palace-the-hague/ (accessed 5 February 2016).

158 Council of the European Union, *Council Regulation (EC) No. 428/2009 on Setting up a Community Regime for the Control of Exports, Transfer, Brokering and Transit of Dual-use Items* (Brussels, 5 May 2009).

159 There is currently no internationally valid definition of cyberspace. Using the Tallinn Manual, NATO's cyberdefence centre has collected a list of the definitions commonly used within the Alliance. CCDCOE, *Cyber Definitions*, https://ccdcoe.org/cyber-definitions.html (accessed 5 February 2016).

160 Julie Hirschfeld Davis and David E. Sanger, "Obama and Xi Jinping of China Agree to Steps on Cybertheft", *The New York Times*, 25 September 2015, http://www.nytimes.com/2015/09/26/world/asia/xi-jinping-white-house.html?_r=0 (accessed 5 February 2016).

(Improving) The Implementation of Due Diligence

Germany's international cyber policy needs a strategic reorientation that takes German and European interests into account. As a European middle-size power, Germany will only be able to find this new focus in a perspective that is in keeping with its integration in European Union, democratic values and firm commitment to civilian forms of politics. The due diligence norm lends itself to that. It expresses the cooperative and global character of a good international cyber and cybersecurity policy, without concealing its domestic foundations. Modern (cyber) foreign and security policies are always also domestic policies.

Germanys has started to implement the due diligence principle in its cyber policy. The fundamental idea of due diligence is that states bear responsibility for threats that emanate from their territory and must do everything in their power in cooperation with other EU states and allies to prevent damage to third parties. Developments in German cybersecurity structures are already taking great strides in this direction. They are at least partly coordinated with the EU and bring together a great number of interested parties. In digital industrial policy cooperation between state and private actors with the aim of pooling professional expertise is needed to give due diligence greater weight. In both areas, there is a marked precedence of civilian over military approaches.

Nevertheless, a series of starting-points remain for improving Germany's International and European cyber policy and cyberdefence policy:

First: The norm of due diligence must be lastingly enforced in international relations. For the time being, it merely has the status of a controversial legal standard and is not included as a binding regulation in bilateral and multilateral agreements. In the final report of the fourth round of UN GGE negotiations, the represented states commit to stopping attacks that emanate from their territories and also commit to not deliberately damaging other countries' critical infrastructure or IT emergency teams. The agreement between the US and China on jointly fighting cybercrime and on outlawing industrial espionage is also a promising step that can serve as a model for bilateral agreements between other countries. Here, it will be important to work politically towards a general recognition of due diligence and also to create the necessary institutional structures in the medium term to guarantee that the norm is being applied effectively. The German Ministry of Foreign Affairs plays a leading role in coordinating an international cyber policy and cyberdefence policy at the EU level. It is the only department that rises above the sectional perspectives of individual policy areas; and as a cross-ministerial responsibility.

Germany's international cyber policy and cybersecurity policy should be formulated even more strongly inside EU structures. Only because of the European single market is Germany able to act with the necessary vigour on the international stage. A promising starting-point is the Friends of the Presidency Group (FoP) on Cyber Issues. It was created in 2013 to support the implementation of the EU cybersecurity strategy. In FoP, the various cyber topics are coordinated horizontally at the EU level. While the working group has so far only been set up for three years at a time, it has already become the most important hub for coordinating national interests in EU cyber policy.

Second: Only a close cooperation between the EU and USA is the adequate framework for drafting international norms. Where they agree, they have enough political influence to tilt the scales towards a more effective enforcement of due diligence. What is urgently needed now is a transatlantic initiative on the attribution problem, meaning the difficulty of unequivocally attributing cyber attacks to an actor. States frequently use this difficulty as a way out of due diligence by shifting the blame onto third parties. In line with the TTIP negotiations, both an economic data transfer and a bilateral agreement on mutual legal assistance need to be agreed on. The EU's General Data Protection Regulation should quickly be complemented by Privacy Shield agreed by the EU and the US that meets the legal criteria formulated by the ECJ. Implementation of the the Privacy Shield should take into account the legal reservations expressed in the ECJ's decision of October 2015. This is the only basis for giving companies and consumers the necessary legal certainty. With its General Data Protection Regulation, the EU has defused the problem of European citizens' data being stored and evaluated according to US law. How-

ever, it has also set a questionable precedent of extra-territorial applicability of its legislation – despite having previously criticised the US for such practices. In practice, global companies now store any data of European citizens in Europe to prevent clashing with EU law. With this decision, the EU will applys its own law on others' sovereign territory. Extra-territorial effects of national law contradict the principle of due diligence obligations. States such as the US and China are likely to have fewer scruples in future about passing legal provisions with extra-territorial effect. This could result in a collision course for different national legal systems, which would encourage the fragmentation of the global economic space and the Internet. The Privacy Shield for data transfer and the transatlantic agreement on data protection in criminal cases are therefore vital steps in the effort to stop this process.

Third: Due diligence obligations should be imposed on those states which have been attacked, on whose territory the servers are located, or over whose data cables attacks are carried out. The density of these obligations should depend on the ability of the states in questions to exert influence and on their ICT capacities. It also seems sensible to strengthen the substantive criminal law and use it for deterrence. Moreover, IT forensics in particular should be expanded so that perpetrators of cyber attacks become easier to identify. Non-state actors should be called on to participate actively. Where companies are forced to break the law because of differences in national legal standards (for instance, on the one hand, a state's demand for information that must be complied with, and on the other hand, a prohibition on handing out data for data protection reasons), the states involved do not live up to the principle of the rule of law. Given the experience of European integration, it would be advisable to confer competences on a supranational jurisdiction along the lines of the European Court of Justice or courts of arbitration, so as to enforce due diligence better on this point. This would also reduce legal uncertainty for companies. On the other hand, it must be possible to force companies to make their software products more secure. At the very least, the criteria for transparency, testing and certification must be made more stringent at least on the EU level within ENISA.

Fourth: The growing complexity of IT-protected weapons systems and the high quality that detected cyber attacks now attain demand much cybersecurity know-how. Moreover, the defence industry needs to take data security into account at the design stage of any system architecture. It therefore stands to reason that manufacturers should be included in the further development and use of cyberdefence systems. However, this should be coordinated at the European level, approved by politically independent or parliamentary decisions, and remain committed to an exclusively defensive military logic. Otherwise, such conduct would run counter to due diligence and would also break with the tradition of military restraint in foreign and security policy. The required inclusiveness in all issues of international cyber policy and cybersecurity policy also means that the German Federal Parliament must be duly involved. Should the German armed forces be empowered to use digital attacks as part of their cyberdefence, the political change of course that might be required for this would need to be debated in Parliament. A robust security policy presupposes social resilience, which can only be created through public debate. This also includes carrying out a reality check on the parliamentary-approval requirement for cyber operations by the German armed forces. It will be the Parliament's task to create effective structures for parliamentary oversight.

List of Abbreviations

AA	Federal Ministry for Foreign Affairs
BAAINBw	Federal Office of Bundeswehr Equipment, Information Technology and In-Service Support
BBK	Federal Office for Civil Protection and Disaster Assistance
BfV	Federal Office for the Protection of the Constitution
BKA	Federal Criminal Police Office
BMBF	Federal Ministry of Education and Research
BMI	Federal Ministry of the Interior
BMVg	Federal Ministry of Defence
BMVI	Federal Ministry for Traffic and Digital Infrastructure
BMWi	Federal Ministry for Economic Affairs and Energy
BND	Federal Intelligence Service
BPol	Federal Police
BSI	Federal Office of Information Security
CAPS	Child Abuse Prevention System
CCDCOE	Cooperative Cyber Defence Centre of Excellence (NATO)
CEF	Connecting Europe Facility
CERT	Computer Emergency Response Team
CERT-Bund	Computer Emergency Response Team of the German Federal Administration
CERTBw	Computer Emergency Response Team of the German armed forces
CIRK	Cyberspace and information-space command
CNA	Computer network attacks
CND	Computer network defence
CNE	Computer network exploitation
CNO	Computer network operation
COMPACT	*C*ivic Responsibilities, *0*ne Unfragmented Resource, *M*ultistakeholder Approach to *P*romote Democracy and Human Rights, Sound Technological *A*rchitecture, *C*onfidence and *T*ransparent Governance
CSBM	Confidence- and security-building measures
CSDP	Common Security and Defence Policy
CSIRT	Computer Security Incident Response Team
ECJ	European Court of Justice
EEAS	European External Action Service
EFTA	European Free Trade Association
EGC	European Government CERTs Group
ENISA	European Network and Information Security Agency
EU	European Union
Eurojust	European Union's Judicial Cooperation Unit
Europol	European Police Office
FIRST	Forum for Incident Response and Security Teams
FoP	Friends of the Presidency Group on Cyber Issues
GDPR	General Data Protection Regulation (EU)
GGE	Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN)
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and communication technology
IGF	Internet Governance Forum
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information technology
IWWN	International Watch and Warning Network
KSA	Kommando Strategische Aufklärung – strategic reconnaissance commando
MAD	Military Counterintelligence Service
MLA	mutual legal assistance agreement
NIS	Network and Information Security
NIST	National Institute of Standards (USA)
NSA	National Security Agency
OECD	Organisation for Economic Co-operation and Development
OSCE	Organization for Security and Cooperation in Europe
PKGr	Parlamentary oversight committee
PPP	Public-Private Partnership
SIGINT	Signals Intelligence
SIT	Strategic Initiative Technology
SME	Small and medium enterprises
SWP	Stiftung Wissenschaft und Politik
TA	Signal intelligence
TFTP	Terrorist Finance Tracking Programme
TTIP	Transatlantic Trade and Investment Partnership
UN	United Nations
UP KRITIS	Implementation plan for (critical) infrastructure
WEF	World Economic Forum
WSIS	World Summit on the Information Society
ZKA	Customs Investigation Bureau